XS1920 Series

10 GbE Web-managed Switches

Version 4.20
Edition 2, 1/2015

User's Guide

Default Login Details	
LAN IP Address	http://192.168.1.1
User Name	admin
Password	1234

Copyright © 2015 ZyXEL Communications Corporation

IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

This is a User's Guide for a series of products. Not all products support all firmware features. Screenshots and graphics in this book may differ slightly from your product due to differences in your product firmware or your computer operating system. Every effort has been made to ensure that the information in this manual is accurate.

Contents Overview

User's Guide **17**

Getting to Know Your Switch 18
Hardware Installation and Connection 22
Hardware Panels 25

Technical Reference **31**

The Web Configurator 32
Initial Setup Example 39
Tutorials 43
ZON Utility, ZON Neighbor Management and Port Status 51
Basic Setting 58
VLAN 86
Static MAC Forward Setup 108
Static Multicast Forward Setup 110
Filtering 113
Spanning Tree Protocol 115
Bandwidth Control 134
Broadcast Storm Control 136
Mirroring 138
Link Aggregation 140
Port Authentication 148
Port Security 156
Time Range 160
Classifier 162
Policy Rule 171
Queuing Method 175
Multicast 178
AAA 201
IP Source Guard 212
Loop Guard 235
Layer 2 Protocol Tunneling 239
PPPoE 243
Error Disable 252
MAC Pinning 258
Private VLAN 260
Green Ethernet 264
Link Layer Discovery Protocol (LLDP) 266
Static Route 291

Differentiated Services 296
DHCP 300
ARP Setup 313
Maintenance 318
Access Control 327
Diagnostic 344
Syslog 346
Cluster Management 349
MAC Table 355
IP Table 358
ARP Table 360
Routing Table 362
Path MTU Table 363
Configure Clone 364
Neighbor Table 367
Troubleshooting 369

Table of Contents

Contents Overview **3**

Table of Contents **5**

Part I: User's Guide **17**

Chapter 1
Getting to Know Your Switch **18**

1.1 Introduction 18
1.1.1 Backbone Application 18
1.1.2 Bridging Example 19
1.1.3 High Performance Switching Example 19
1.1.4 IEEE 802.1Q VLAN Application Examples 20
1.2 Ways to Manage the Switch 21
1.3 Good Habits for Managing the Switch 21

Chapter 2
Hardware Installation and Connection **22**

2.1 Installation Scenarios 22
2.2 Desktop Installation Procedure 22
2.3 Mounting the Switch on a Rack 22
2.3.1 Rack-mounted Installation Requirements 22
2.3.2 Attaching the Mounting Brackets to the Switch 23
2.3.3 Mounting the Switch on a Rack 23

Chapter 3
Hardware Panels **25**

3.1 Front Panel 25
3.1.1 Gigabit Ethernet Ports 25
3.1.2 SFP/SFP+ Slots 26
3.2 Rear Panel 28
3.2.1 Power Connector 28
3.3 LEDs 29
3.4 Reset to Factory Defaults 29

Part II: Technical Reference **31**

Chapter 4
The Web Configurator 32

4.1 Overview 32
4.2 System Login 32
4.3 The Status Screen 33
4.3.1 Change Your Password 37
4.4 Saving Your Configuration 37
4.5 Switch Lockout 37
4.6 Resetting the Switch 38
4.7 Logging Out of the Web Configurator 38
4.8 Help 38

Chapter 5
Initial Setup Example 39

5.1 Overview 39
5.1.1 Creating a VLAN 39
5.1.2 Setting Port VID 40
5.2 Configuring Switch Management IP Address 41

Chapter 6
Tutorials 43

6.1 Overview 43
6.2 How to Use DHCP Snooping on the Switch 43
6.3 How to Use DHCP Relay on the Switch 47
6.3.1 DHCP Relay Tutorial Introduction 47
6.3.2 Creating a VLAN 47
6.3.3 Configuring DHCP Relay 49
6.3.4 Troubleshooting 50

Chapter 7
ZON Utility, ZON Neighbor Management and Port Status 51

7.1 Overview 51
7.1.1 What You Can Do 51
7.2 ZyXEL One Network (ZON) Utility Screen 51
7.3 Neighbor Screen 52
7.4 Port Status Summary 53
7.4.1 Status: Port Details 54

Chapter 8
Basic Setting 58

8.1 Overview 58
8.1.1 What You Can Do 58
8.2 System Information 58

8.3 General Setup 60
8.4 Introduction to VLANs 62
8.5 Switch Setup Screen 63
8.6 IP Setup 65
8.6.1 IP Status 65
8.6.2 IP Status Details 65
8.6.3 IP Configuration 67
8.7 Port Setup 69
8.8 Interface Setup 71
8.9 IPv6 72
8.9.1 IPv6 Interface Status 72
8.9.2 IPv6 Configuration 75
8.9.3 IPv6 Global Setup 76
8.9.4 IPv6 Interface Setup 76
8.9.5 IPv6 Link-Local Address Setup 77
8.9.6 IPv6 Global Address Setup 78
8.9.7 IPv6 Neighbor Discovery Setup 79
8.9.8 IPv6 Router Discovery Setup 80
8.9.9 IPv6 Prefix Setup 82
8.9.10 IPv6 Neighbor Setup 83
8.9.11 DHCPv6 Client Setup 84

Chapter 9
VLAN 86

9.1 Overview 86
9.1.1 What You Can Do 86
9.1.2 What You Need to Know 86
9.2 VLAN Status 89
9.2.1 VLAN Details 90
9.3 Private VLAN Status 91
9.4 VLAN Configuration 92
9.5 Configure a Static VLAN 92
9.6 Configure VLAN Port Settings 94
9.7 Subnet Based VLANs 96
9.7.1 Configuring Subnet Based VLAN 97
9.8 Protocol Based VLANs 98
9.8.1 Configuring Protocol Based VLAN 99
9.9 Voice VLAN 100
9.10 MAC-based VLAN 102
9.11 Port-based VLAN Setup 103
9.12 Port-based VLAN 104
9.13 Technical Reference 106
9.13.1 Create an IP-based VLAN Example 106

Chapter 10
Static MAC Forward Setup 108

10.1 Overview 108
10.1.1 What You Can Do 108
10.2 Configuring Static MAC Forwarding 108

Chapter 11
Static Multicast Forward Setup 110

11.1 Static Multicast Forward Setup Overview 110
11.1.1 What You Can Do 110
11.1.2 What You Need To Know 110
11.2 Configuring Static Multicast Forwarding 111

Chapter 12
Filtering 113

12.1 Filtering Overview 113
12.1.1 What You Can Do 113
12.2 Configure a Filtering Rule 113

Chapter 13
Spanning Tree Protocol 115

13.1 Spanning Tree Protocol Overview 115
13.1.1 What You Can Do 115
13.1.2 What You Need to Know 115
13.2 Spanning Tree Protocol Status Screen 118
13.3 Spanning Tree Configuration 118
13.4 Configure Rapid Spanning Tree Protocol 119
13.4.1 Rapid Spanning Tree Protocol Status 121
13.5 Configure Multiple Rapid Spanning Tree Protocol 122
13.5.1 Multiple Rapid Spanning Tree Protocol Status 124
13.6 Configure Multiple Spanning Tree Protocol 125
13.6.1 Multiple Spanning Tree Port Configuration 128
13.6.2 Multiple Spanning Tree Protocol Status 129
13.7 Technical Reference 131
13.7.1 MSTP Network Example 131
13.7.2 MST Region 132
13.7.3 MST Instance 133
13.7.4 Common and Internal Spanning Tree (CIST) 133

Chapter 14
Bandwidth Control 134

14.1 Overview 134
14.1.1 What You Can Do 134

14.2 Bandwidth Control Setup 134

Chapter 15
Broadcast Storm Control 136

15.1 Broadcast Storm Control Overview 136
15.1.1 What You Can Do 136
15.2 Broadcast Storm Control Setup 136

Chapter 16
Mirroring 138

16.1 Mirroring Overview 138
16.1.1 What You Can Do 138
16.2 Port Mirroring Setup 138

Chapter 17
Link Aggregation 140

17.1 Overview 140
17.1.1 What You Can Do 140
17.1.2 What You Need to Know 140
17.2 Link Aggregation Status 141
17.3 Link Aggregation Setting 142
17.4 Link Aggregation Control Protocol 144
17.5 Technical Reference 146
17.5.1 Static Trunking Example 146

Chapter 18
Port Authentication 148

18.1 Port Authentication Overview 148
18.1.1 What You Need to Know 148
18.1.2 MAC Authentication 149
18.2 Port Authentication Configuration 150
18.3 Activate IEEE 802.1x Security 150
18.3.1 Guest VLAN 151
18.3.2 Activate MAC Authentication 153

Chapter 19
Port Security 156

19.1 Port Security Overview 156
19.1.1 What You Can Do 156
19.2 Port Security Setup 156
19.3 VLAN MAC Address Limit 158

Chapter 20
Time Range 160

20.1 About Time Range 160
20.2 Time Range Setup 160

Chapter 21
Classifier 162

21.1 Overview 162
21.1.1 What You Can Do 162
21.1.2 What You Need to Know 162
21.2 Classifier Status 162
21.3 Classifier Configuration 163
21.3.1 Viewing and Editing Classifier Configuration 167
21.3.2 Classifier Global Setting 168
21.4 Classifier Example 169

Chapter 22
Policy Rule 171

22.1 Policy Rules Overview 171
22.1.1 What You Can Do 171
22.2 Configuring Policy Rules 171
22.2.1 Viewing and Editing Policy Configuration 174

Chapter 23
Queuing Method 175

23.1 Queuing Method Overview 175
23.1.1 What You Can Do 175
23.1.2 What You Need to Know 175
23.2 Configuring Queuing 176

Chapter 24
Multicast 178

24.1 Multicast Overview 178
24.1.1 What You Can Do 178
24.1.2 What You Need to Know 178
24.2 Multicast Setup 182
24.3 IPv4 Multicast Status 182
24.3.1 IGMP Snooping 183
24.4 IGMP Snooping VLAN 185
24.4.1 IGMP Filtering Profile 187
24.5 IPv6 Multicast Status 188
24.5.1 MLD Snooping-proxy 189
24.5.2 MLD Snooping-proxy VLAN 189
24.5.3 MLD Snooping-proxy VLAN Port Role Setting 191
24.5.4 MLD Snooping-proxy VLAN Filtering 193

24.5.5 MLD Snooping-proxy VLAN Filtering Profile 194
24.6 General MVR Configuration 195
24.6.1 MVR Group Configuration 197
24.6.2 MVR Configuration Example 199

Chapter 25
AAA 201

25.1 AAA Overview 201
25.1.1 What You Can Do 201
25.1.2 What You Need to Know 201
25.2 AAA Screens 202
25.3 RADIUS Server Setup 202
25.4 TACACS+ Server Setup 204
25.5 AAA Setup 206
25.6 Technical Reference 208
25.6.1 Vendor Specific Attribute 208
25.6.2 Supported RADIUS Attributes 210
25.6.3 Attributes Used for Authentication 210

Chapter 26
IP Source Guard 212

26.1 Overview 212
26.1.1 What You Can Do 212
26.1.2 What You Need to Know 213
26.2 IP Source Guard 213
26.3 IP Source Guard Static Binding 214
26.4 DHCP Snooping 215
26.5 DHCP Snooping Configure 218
26.5.1 DHCP Snooping Port Configure 220
26.5.2 DHCP Snooping VLAN Configure 221
26.5.3 DHCP Snooping VLAN Port Configure 222
26.6 ARP Inspection Status 223
26.7 ARP Inspection VLAN Status 224
26.8 ARP Inspection Log Status 225
26.9 ARP Inspection Configure 227
26.9.1 ARP Inspection Port Configure 228
26.9.2 ARP Inspection VLAN Configure 230
26.10 Technical Reference 231
26.10.1 DHCP Snooping Overview 231
26.10.2 ARP Inspection Overview 233

Chapter 27
Loop Guard 235

27.1 Loop Guard Overview 235
27.1.1 What You Can Do 235
27.1.2 What You Need to Know 235
27.2 Loop Guard Setup 237

Chapter 28
Layer 2 Protocol Tunneling 239

28.1 Layer 2 Protocol Tunneling Overview 239
28.1.1 What You Can Do 239
28.1.2 What You Need to Know 239
28.2 Configuring Layer 2 Protocol Tunneling 240

Chapter 29
PPPoE 243

29.1 PPPoE Intermediate Agent Overview 243
29.1.1 What You Can Do 243
29.1.2 What You Need to Know 243
29.2 The PPPoE Screen 246
29.3 PPPoE Intermediate Agent 246
29.3.1 PPPoE IA Per-Port 247
29.3.2 PPPoE IA Per-Port Per-VLAN 249
29.3.3 PPPoE IA for VLAN 250

Chapter 30
Error Disable 252

30.1 Error Disable Overview 252
30.2 The Error Disable Screens Overview 252
30.3 Error-Disable Status 252
30.4 CPU Protection Configuration 254
30.5 Error-Disable Detect Configuration 255
30.6 Error-Disable Recovery Configuration 256

Chapter 31
MAC Pinning 258

31.1 MAC Pinning Overview 258
31.2 MAC Pinning Configuration 258

Chapter 32
Private VLAN 260

32.1 Private VLAN Overview 260
32.1.1 Configuration 262

Chapter 33
Green Ethernet 264

33.1 Green Ethernet Overview 264
33.2 Configuring Green Ethernet 264

Chapter 34
Link Layer Discovery Protocol (LLDP) 266

34.1 LLDP Overview 266
34.2 LLDP-MED Overview 267
34.3 LLDP Screens 268
34.4 LLDP Local Status 269
34.4.1 LLDP Local Port Status Detail 270
34.5 LLDP Remote Status 274
34.5.1 LLDP Remote Port Status Detail 275
34.6 LLDP Configuration 281
34.6.1 LLDP Configuration Basic TLV Setting 283
34.6.2 LLDP Configuraion Basic Org-specific TLV Setting 284
34.7 LLDP-MED Configuration 285
34.8 LLDP-MED Network Policy 286
34.9 LLDP-MED Location 287

Chapter 35
Static Route 291

35.1 Static Route Overview 291
35.1.1 What You Can Do 291
35.2 Static Routing 291
35.3 Configuring Static Routing 292
35.4 Configuring IPv6 Static Routing 294

Chapter 36
Differentiated Services 296

36.1 Differentiated Services Overview 296
36.1.1 What You Can Do 296
36.1.2 What You Need to Know 296
36.2 Activating DiffServ 297
36.3 DSCP-to-IEEE 802.1p Priority Settings 298
36.3.1 Configuring DSCP Settings 299

Chapter 37
DHCP 300

37.1 DHCP Overview 300
37.1.1 What You Can Do 300
37.1.2 What You Need to Know 300
37.2 DHCP Configuration 301
37.3 DHCPv4 Status 302

37.4 DHCPv4 Relay 302
37.4.1 DHCPv4 Relay Agent Information 302
37.4.2 DHCPv4 Option 82 Profile 303
37.4.3 Configuring DHCPv4 Global Relay 305
37.4.4 DHCPv4 Global Relay Port Configure 306
37.4.5 Global DHCP Relay Configuration Example 307
37.5 Configuring DHCPv4 VLAN Settings 308
37.5.1 DHCPv4 VLAN Port Configure 309
37.5.2 Example: DHCP Relay for Two VLANs 310
37.6 DHCPv6 Relay 311

Chapter 38
ARP Setup 313

38.1 ARP Overview 313
38.1.1 How ARP Works 313
38.1.2 ARP Learning Mode 313
38.2 ARP Setup 315
38.2.1 ARP Learning 315
38.2.2 Static ARP 316

Chapter 39
Maintenance 318

39.1 Overview 318
39.2 The Maintenance Screen 318
39.2.1 Firmware Upgrade 319
39.2.2 Restore a Configuration File 320
39.2.3 Backup a Configuration File 321
39.2.4 Erase Running-Configuration 321
39.2.5 Save Configuration 322
39.2.6 Reboot System 322
39.2.7 Factory Default 322
39.3 Tech-Support 323
39.4 Technical Reference 324
39.4.1 FTP Command Line 324
39.4.2 Filename Conventions 324
39.4.3 FTP Command Line Procedure 325
39.4.4 GUI-based FTP Clients 325
39.4.5 FTP Restrictions 326

Chapter 40
Access Control 327

40.1 Access Control Overview 327
40.1.1 What You Can Do 327

40.2 The Access Control Main Screen 327
40.3 Configuring SNMP 328
40.3.1 Configuring SNMP Trap Group 329
40.3.2 Enabling/Disabling Sending of SNMP Traps on a Port 330
40.3.3 Configuring SNMP User 331
40.4 Setting Up Login Accounts 332
40.5 Service Port Access Control 334
40.6 Remote Management 335
40.7 Technical Reference 336
40.7.1 About SNMP 336
40.7.2 Introduction to HTTPS 339

Chapter 41
Diagnostic 344

41.1 Overview 344
41.2 Diagnostic 344

Chapter 42
Syslog 346

42.1 Syslog Overview 346
42.1.1 What You Can Do 346
42.2 Syslog Setup 346
42.3 Syslog Server Setup 347

Chapter 43
Cluster Management 349

43.1 Cluster Management Overview 349
43.1.1 What You Can Do 350
43.2 Cluster Management Status 350
43.3 Clustering Management Configuration 351
43.4 Technical Reference 353
43.4.1 Cluster Member Switch Management 353

Chapter 44
MAC Table 355

44.1 MAC Table Overview 355
44.1.1 What You Can Do 355
44.1.2 What You Need to Know 355
44.2 Viewing the MAC Table 356

Chapter 45
IP Table 358

45.1 IP Table Overview 358

45.2 Viewing the IP Table 359

Chapter 46
ARP Table 360

46.1 Overview 360
46.1.1 What You Can Do 360
46.1.2 What You Need to Know 360
46.2 Viewing the ARP Table 360

Chapter 47
Routing Table 362

47.1 Overview 362
47.2 Viewing the Routing Table Status 362

Chapter 48
Path MTU Table 363

48.1 Path MTU Overview 363
48.2 Viewing the Path MTU Table 363

Chapter 49
Configure Clone 364

49.1 Overview 364
49.2 Configure Clone 364

Chapter 50
Neighbor Table 367

50.1 IPv6 Neighbor Table Overview 367
50.2 Viewing the IPv6 Neighbor Table 367

Chapter 51
Troubleshooting 369

51.1 Power, Hardware Connections, and LEDs 369
51.2 Switch Access and Login 370
51.3 Switch Configuration 372

Appendix A Customer Support 373

Appendix B Common Services 379

Appendix C IPv6 382

Appendix D Legal Information 390

Index 395

PART I
User's Guide

1

Getting to Know Your Switch

1.1 Introduction

This chapter introduces the main features and applications of the Switch. The XS1920 Series consist of the following models at the time of writing:

- XS1920-12

The Switch is a 10G Ethernet web-managed switch with layer-2, layer-3, and layer-4 features.

With its built-in web configurator, including the ZyXEL One Network (ZON) Neighbor Management feature (Section 7.2 on page 51), viewing, managing and configuring the Switch and its neighboring devices is easy. The Switch can also be managed via third-party SNMP management.

ZyXEL One Network (ZON) Utility is a tool that lets set up and maintain network devices in a simple and efficient way. You can download the ZON Utility at www.zyxel.com and install it on a computer. For more information on the ZON Utility see Section 7.2 on page 51.

The following table describes the port features of the 10G Switch. 100Mbps connections are not guaranteed.

Table 1 Port Features

SWITCH MODEL	PORT FEATURES
XS1920-12	• 12 10 Gbps Ethernet ports • 2 1G/10G SFP+fiber ports

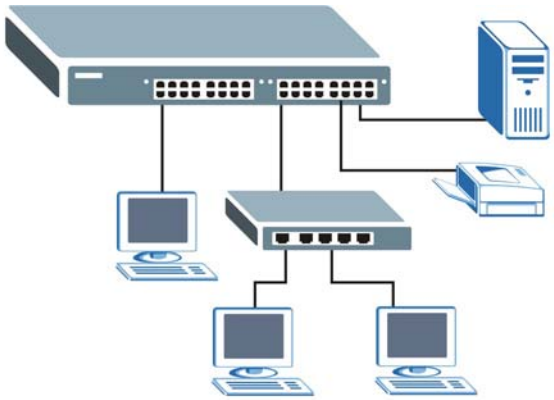
The next section shows a few examples of using the Switch in various network environments.

1.1.1 Backbone Application

The Switch is an ideal solution for small networks where rapid growth can be expected in the near future. The Switch can be used standalone for a group of heavy traffic users. You can connect computers and servers directly to the Switch's port or connect other switches to the Switch.

In this example, all computers can share high-speed applications on the server. To expand the network, simply add more networking devices such as switches, routers, computers, print servers etc.

Figure 1 Backbone Application

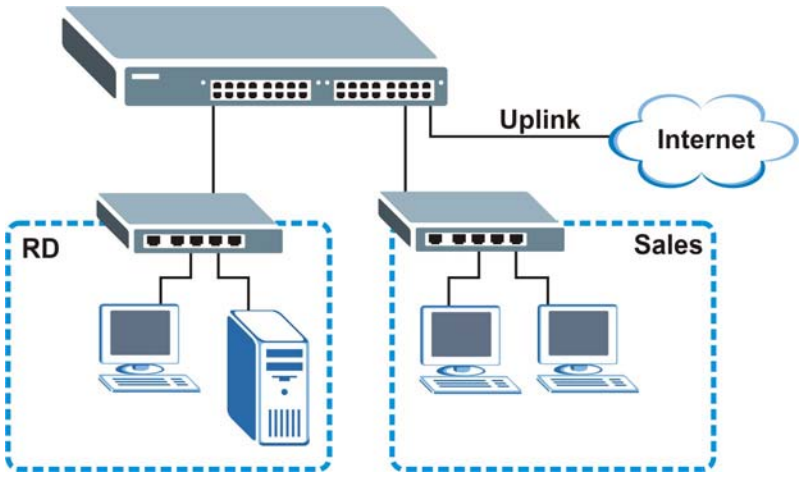


1.1.2 Bridging Example

In this example, the Switch connects different company departments (**RD** and **Sales**) to the corporate backbone. It can alleviate bandwidth contention and eliminate server and network bottlenecks. All users that need high bandwidth can connect to high-speed department servers via the Switch. You can provide a super-fast uplink connection by using a Gigabit Ethernet/mini-GBIC port on the Switch.

Moreover, the Switch eases supervision and maintenance by allowing network managers to centralize multiple servers at a single location.

Figure 2 Bridging Application



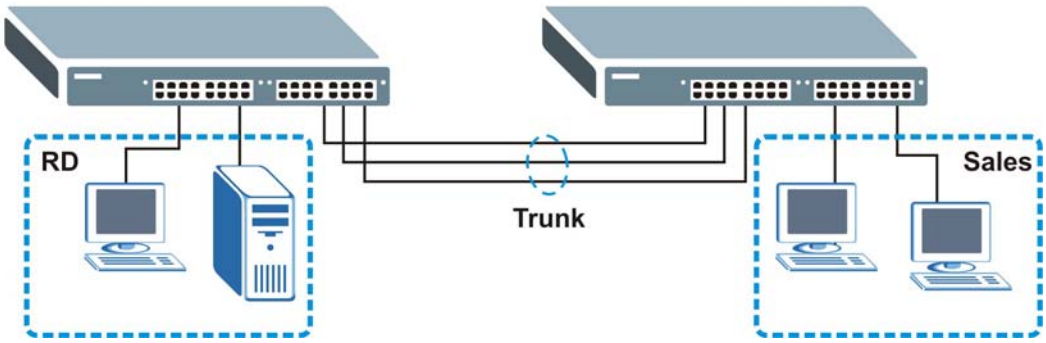
1.1.3 High Performance Switching Example

The Switch is ideal for connecting two networks that need high bandwidth. In the following example, use trunking to connect these two networks.

Switching to higher-speed LANs such as ATM (Asynchronous Transmission Mode) is not feasible for most people due to the expense of replacing all existing Ethernet cables and adapter cards, restructuring your network and complex maintenance. The Switch can provide the same bandwidth

as ATM at much lower cost while still being able to use existing adapters and switches. Moreover, the current LAN structure can be retained as all ports can freely communicate with each other.

Figure 3 High Performance Switched Workgroup Application



1.1.4 IEEE 802.1Q VLAN Application Examples

A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Stations on a logical network belong to one group. A station can belong to more than one group. With VLAN, a station cannot directly talk to or hear from stations that are not in the same group(s) unless such traffic first goes through a router.

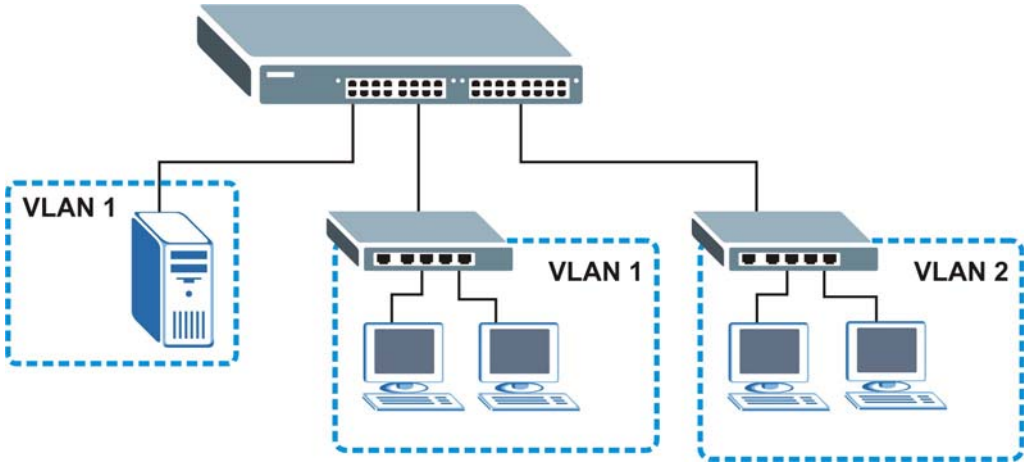
For more information on VLANs, refer to Chapter 9 on page 86.

1.1.4.1 Tag-based VLAN Example

Ports in the same VLAN group share the same frame broadcast domain thus increase network performance through reduced broadcast traffic. VLAN groups can be modified at any time by adding, moving or changing ports without any re-cabling.

Shared resources such as a server can be used by all ports in the same VLAN as the server. In the following figure only ports that need access to the server need to be part of VLAN 1. Ports can belong to other VLAN groups too.

Figure 4 Shared Server Using VLAN Example



1.2 Ways to Manage the Switch

Use any of the following methods to manage the Switch.

- Web Configurator. This is recommended for everyday management of the Switch using a (supported) web browser. See Chapter 4 on page 32.
- FTP. Use FTP for firmware upgrades and configuration backup/restore. See Section 39.4.1 on page 324.
- SNMP. The Switch can be monitored by an SNMP manager. See Section 40.5 on page 334.
- Cluster Management. Cluster Management allows you to manage multiple switches through one switch, called the cluster manager. See Chapter 43 on page 349.

1.3 Good Habits for Managing the Switch

Do the following things regularly to make the Switch more secure and to manage the Switch more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the Switch to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the Switch. You could simply restore your last configuration. See Section 3.4 on page 29 for how to reset the Switch.

2

Hardware Installation and Connection

2.1 Installation Scenarios

This chapter shows you how to install and connect the Switch.

The Switch can be placed on a desktop or rack-mounted on a standard EIA rack. Use the rubber feet in a desktop installation and the brackets in a rack-mounted installation.

Note: For proper ventilation, allow at least 4 inches (10 cm) of clearance at the front and 3.4 inches (8 cm) at the back of the Switch. This is especially important for enclosed rack installations.

2.2 Desktop Installation Procedure

1 Make sure the Switch is clean and dry.

2 Set the Switch on a smooth, level surface strong enough to support the weight of the Switch and the connected cables. Make sure there is a power outlet nearby.

3 Make sure there is enough clearance around the Switch to allow air circulation and the attachment of cables and the power cord.

2.3 Mounting the Switch on a Rack

The Switch can be mounted on an EIA standard size, 19-inch rack or in a wiring closet with other equipment. Follow the steps below to mount your Switch on a standard EIA rack using a rack-mounting kit.

2.3.1 Rack-mounted Installation Requirements

- Two mounting brackets.
- Eight M3 flat head screws and a #2 Philips screwdriver.
- Four M5 flat head screws and a #2 Philips screwdriver.

Failure to use the proper screws may damage the unit.

2.3.1.1 Precautions

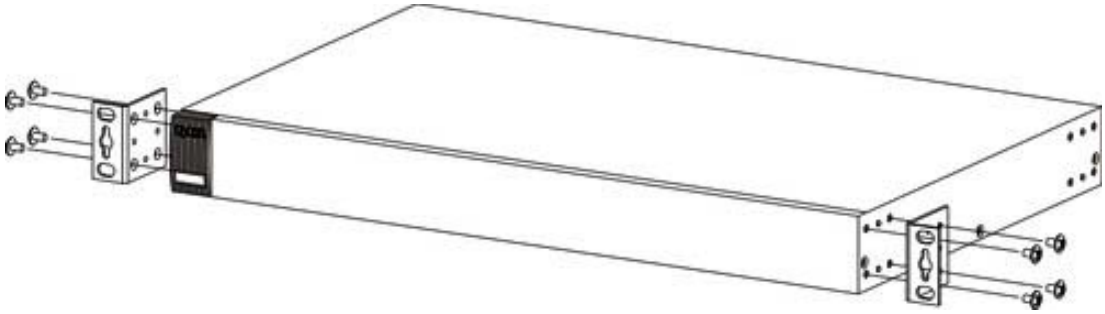
- Make sure the rack will safely support the combined weight of all the equipment it contains.

- Make sure the position of the Switch does not make the rack unstable or top-heavy. Take all necessary precautions to anchor the rack securely before installing the unit.

2.3.2 Attaching the Mounting Brackets to the Switch

1 Position a mounting bracket on one side of the Switch, lining up the four screw holes on the bracket with the screw holes on the side of the Switch.

Figure 5 Attaching the Mounting Brackets



2 Using a #2 Philips screwdriver, install the M3 flat head screws through the mounting bracket holes into the Switch.

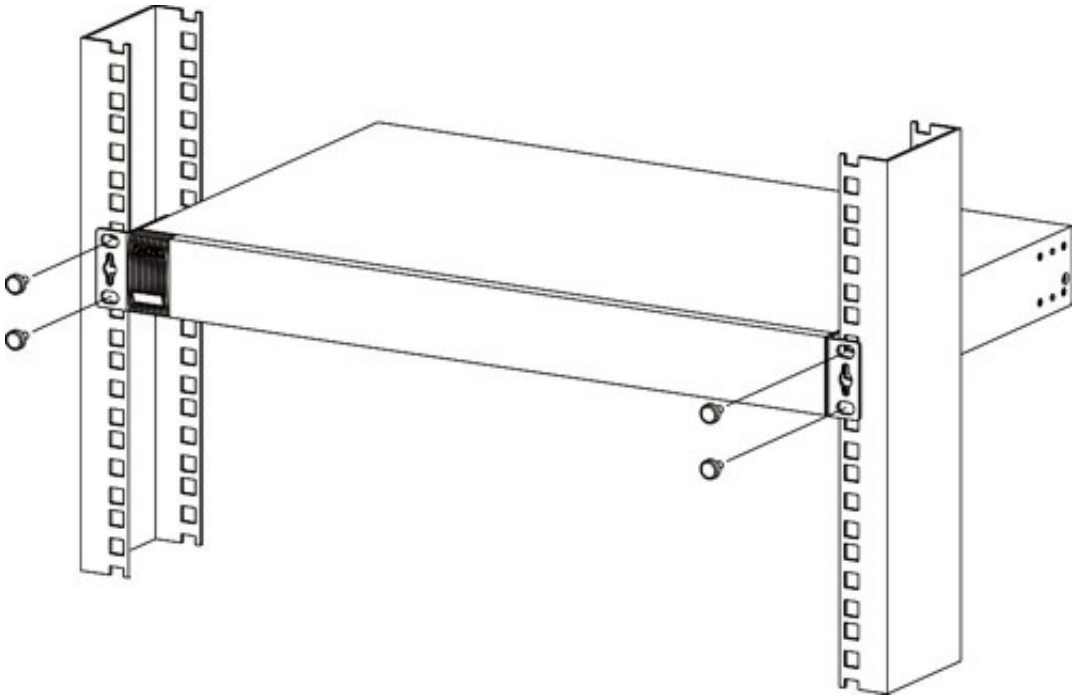
3 Repeat steps 1 and 2 to install the second mounting bracket on the other side of the Switch.

4 You may now mount the Switch on a rack. Proceed to the next section.

2.3.3 Mounting the Switch on a Rack

1 Position a mounting bracket (that is already attached to the Switch) on one side of the rack, lining up the two screw holes on the bracket with the screw holes on the side of the rack.

Figure 6 Mounting the Switch on a Rack



2 Using a #2 Philips screwdriver, install the M5 flat head screws through the mounting bracket holes into the rack.

3 Repeat steps 1 and 2 to attach the second mounting bracket on the other side of the rack.

3

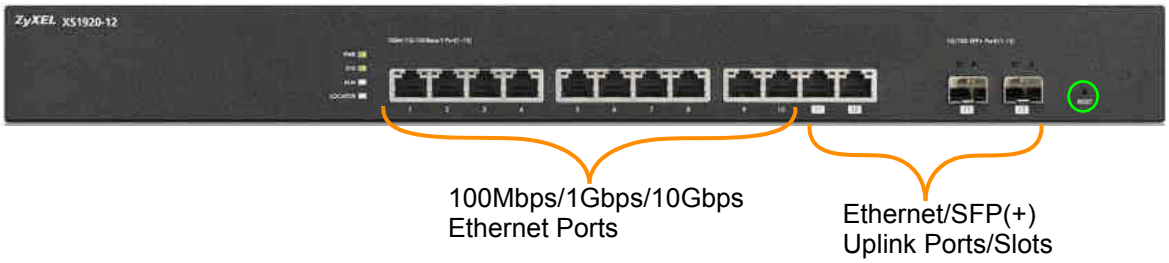
Hardware Panels

This chapter describes the front panel and rear panel of the Switch and shows you how to make the hardware connections.

3.1 Front Panel

The following figures show the front panel of the Switch. See Section 3.3 on page 29 for information on the LEDs. The reset button is also located here as circled below. See Section 3.4 on page 29 for more information on using that.

Figure 7 Front Panel: XS1920-12



The following table describes the ports.

Table 2 Panel Connections

CONNECTOR	DESCRIPTION
Ports 1-10	These are 100Mbps/1Gbps/10Gbps RJ-45 Ethernet ports. Connect these ports to a computer, a hub, an Ethernet switch or router.
Ports 11-12 Ethernet	These are 100Mbps/1Gbps/10Gbps RJ-45 combo uplink ports. The fiber port connection takes priority if the corresponding Ethernet uplink port is also connected. Connect these ports to high-bandwidth backbone network Ethernet switches using 100/1000/10G Base-T cables.
Ports 11-12 Fiber	These are SFP / SFP+ uplink Slots Use SFP transceivers in these slots for fiber-optic to backbone Ethernet switches.

3.1.1 Gigabit Ethernet Ports

Ports 1-10 on the Switch are 100Mbps/1Gbps/10Gbps auto-negotiating, auto-crossover Ethernet ports with full duplex support.

An auto-negotiating port can detect and adjust to the optimum Ethernet speed of the connected device. **Auto-1000M / Full-Duplex** supports Ethernet and fiber connections at 100Mbps or

1000Mbps (1Gbps) full-duplex mode. **Auto-10G / Full-Duplex** supports Ethernet connections at 100Mbps, 1000Mbps or 10Gbps full-duplex mode and 10Gbps only for fiber connections.

When auto-negotiation is turned on, an Ethernet port negotiates with the peer automatically to determine the connection speed. If the peer Ethernet port does not support auto-negotiation or turns off this feature, the Switch determines the connection speed by detecting the signal on the cable. When the Switch's auto-negotiation is turned off, an Ethernet port uses the pre-configured speed when making a connection, thus requiring you to make sure that the settings of the peer Ethernet port are the same in order to connect.

An auto-crossover (auto-MDI/MDI-X) port automatically works with a straight-through or crossover Ethernet cable.

Ports 11 and 12 are Ethernet ports paired with Ports 11 and 12 SGP/SFP+ (fiber) slots. The Switch uses one of either the Ethernet or fiber connection with the fiber connection having priority if the corresponding Ethernet port is also connected. This means that if Port 11 fiber slot and Port 11 Ethernet port are connected at the same time, then Ethernet port 11 will be disabled. Ethernet and fiber ports 12 work the same way.

3.1.1.1 Default Ethernet Negotiation Settings

The factory default negotiation settings for the Ethernet ports on the Switch are:

- Speed: Auto
- Duplex: Full
- Flow control: Off
- Link Aggregation: Disabled

3.1.2 SFP/SFP+ Slots

Fiber ports 11 and 12 are slots for Small Form-Factor Pluggable (Plus) modules, such as an SFP or SFP+ transceivers. SFP+ is an enhanced version of SFP and supports data rates of 10 Gbps. A transceiver is a single unit that houses a transmitter and a receiver. Use a transceiver to connect a fiber-optic cable to the Switch. The Switch does not come with transceivers. You must use transceivers that comply with the Small Form-Factor Pluggable (SFP) Transceiver MultiSource Agreement (MSA). See the SFF committee's INF-8074i specification Rev 1.0 for details.

You can change transceivers while the Switch is operating. You can use different transceivers to connect to Ethernet switches with different types of fiber-optic connectors.

- Type: SFP/SFP+ connection interface
- Connection speed: 1 or 10 Gigabit per second (Gbps)

3.1.2.1 Transceiver Installation

Use the following steps to install a mini-GBIC transceiver (SFP+ module).

1. Insert the transceiver into the slot with the exposed section of PCB board facing down.
2. Press the transceiver firmly until it clicks into place.

3 The Switch automatically detects the installed transceiver. Check the LEDs to verify that it is functioning properly.

4 Close the transceiver's latch (latch styles vary).

5 Connect the fiber optic cables to the transceiver.

Figure 8 Transceiver Installation Example

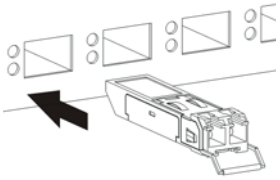
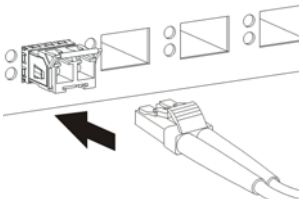


Figure 9 Connecting the Fiber Optic Cables



3.1.2.2 Transceiver Removal

Use the following steps to remove a mini-GBIC transceiver (SFP+ module).

1 Remove the fiber optic cables from the transceiver.

2 Open the transceiver's latch (latch styles vary).

3 Pull the transceiver out of the slot.

Figure 10 Removing the Fiber Optic Cables

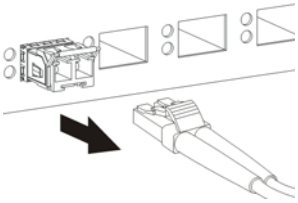


Figure 11 Opening the Transceiver's Latch Example

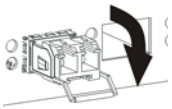
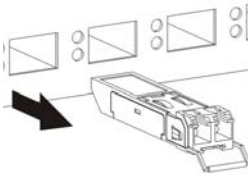


Figure 12 Transceiver Removal Example



3.2 Rear Panel

The following figures show the rear panel of the Switch.

Figure 13 Rear panel: XS1920-12

3.2.1 Power Connector

Note: Make sure you are using the correct power source as shown on the panel.

To connect power to the Switch, insert the female end of the power cord to the AC power receptacle on the rear panel. Connect the other end of the supplied power cord to a power outlet. Make sure that no objects obstruct the airflow of the fans (located on the side of the unit).

3.3 LEDs

After you connect the power to the Switch, view the LEDs to ensure proper functioning of the Switch and as an aid in troubleshooting.

Table 3 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
PWR	Green	On	The system is turned on.
		Off	The system is off or has failed.
SYS	Green	On	The system is on and functioning properly.
		Blinking	The system is rebooting and performing self-diagnostic tests.
		Off	The power is off or the system is not ready/malfunctioning.
ALM	Red	On	A hardware failure, such as high temperature, wrong voltage or abnormal fan speed is detected.
		Off	The system is functioning normally.
LOCATOR	Blue	Blinking	Shows the actual location of the Switch between several devices in a rack.
100M/1G/10G Ethernet Ports		100Mbps connections are not recommended as some legacy 100Mbps devices may have interoperability issues when connected to the combo ports. The LED displays green for successfully connected 100Mbps devices that do not have interoperability issues.	
LNK/ACT (Left)	Green	Blinking	The port is transmitting/receiving to/from a 100 Mbps or a 1000 Mbps (1 Gbps) Ethernet network.
		On	The link to a 100 Mbps or a 1000 Mbps Ethernet network is up.
		Off	The link to an Ethernet network is down.
LNK/ACT (Right)	Blue	Blinking	The port is transmitting/receiving to/from a 10 Gbps Ethernet network.
		On	The link to a 10 Gbps Ethernet network is up.
		Off	The link to an Ethernet network is down.
SFP / SFP+ Slots			
11-12 SFP/SFP+ LNK/ ACT (Left)	Green	On	The uplink port is linking at 1000 Mbps.
		Blinking	The port is transmitting/receiving data 1000 Mbps.
		Off	There is no link or the uplink port is shut down.
11-12 SFP/SFP+ LNK/ ACT (Right)	Blue	On	The uplink port is linking at 10 Gbps.
		Blinking	The port is transmitting/receiving data 10 Gbps.
		Off	There is no link or the uplink port is shut down.

3.4 Reset to Factory Defaults

If you forget your password or cannot access the Web Configurator, you will need to use the Reset button on the device to reload the factory-default configuration file. This means that you will lose all configurations that you had previously and the default Switch IP address, user name and password will be reset to 192.168.1.1, admin and 1234 respectively.

If you backed up an earlier configuration file as advised in Section 1.3 on page 21, you will not have to totally re-configure the Switch after resetting. You can simply restore your last configuration.

Follow the steps below to reset the Switch back to factory defaults.

1 Make sure the SYS LED is steady green (not blinking). Use a pointed instrument such as a pin to access the Reset button on the Switch as shown in Section on page 30.

2 Press the button for more than five seconds until the SYS LED begins to blink and then release it. Wait for the Switch to restart (the SYS LED will be steady green again). This takes up to two minutes.

Note: If you want to access the Switch web configurator again, you may need to change the IP address of your computer to be in the same subnet as that of the default Switch IP address (192.168.1.1).

PART II
Technical Reference

4

The Web Configurator

4.1 Overview

This section introduces the configuration and functions of the web configurator.

The web configurator is an HTML-based management interface that allows easy Switch setup and management via Internet browser. Use one of the following browser versions:

- IE 8 or later
- Chrome 34.0.1847.131 or later
- Firefox 29.0.1 or later
- Opera 21.0 or later
- Safari 5.1.7 or later

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

Note: See your browser help for details on enabling these features.

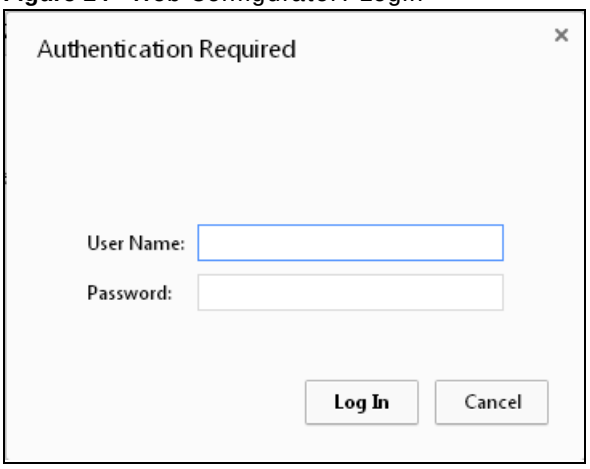
4.2 System Login

1 Start your web browser.

2 Type “http://” and the IP address of the Switch (for example, the default management IP address is 192.168.1.1) in the **Location** or **Address** field. Press [ENTER].

3 The login screen appears. The default username is **admin** and associated default password is **1234**. The date and time display as shown if you have not configured a time server nor manually entered a time and date in the **General Setup** screen.

Figure 14 Web Configurator: Login



4 Click **OK** to view the first web configurator screen.

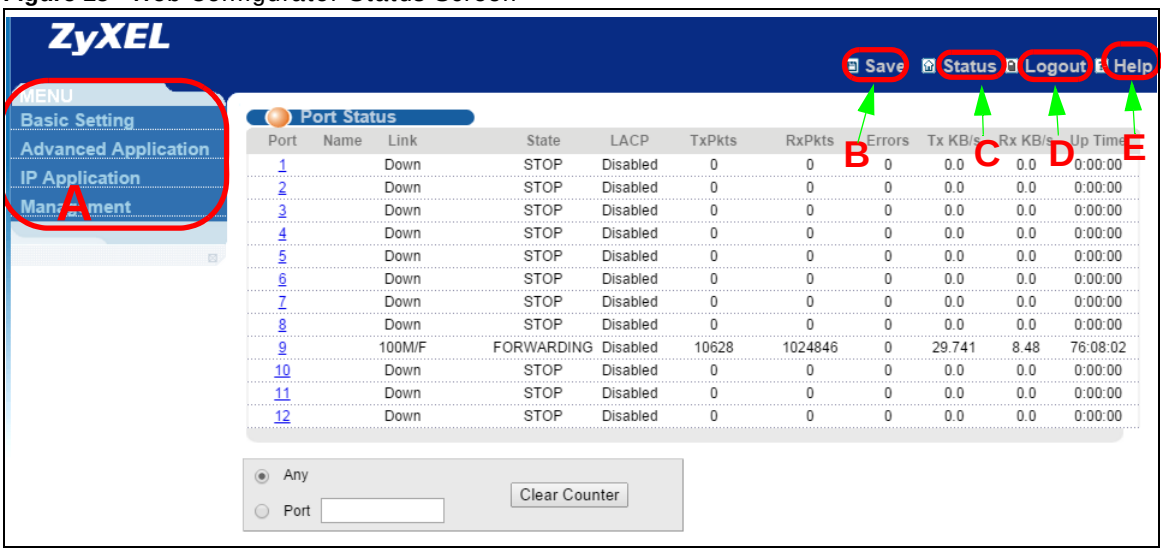
4.3 The Status Screen

The **Status** screen is the first screen that displays when you access the web configurator.

This guide uses PoE model(s) screens as an example. The screens may very slightly for different models.

The following figure shows the navigating components of a web configurator screen.

Figure 15 Web Configurator Status Screen


ZyXEL
Save
Status
Logout
Help
MENU
Basic Setting
Advanced Application
IP Application
Management
A
B
C
D
E
Port Status
Port Name Link State LACP TxPkts RxPkts Errors Tx KB/s Rx KB/s Up Time
1 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
2 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
3 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
4 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
5 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
6 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
7 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
8 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
9 100M/F FORWARDING Disabled 10628 1024846 0 29.741 8.48 76:08:02
10 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
11 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
12 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
Any
Port
Clear Counter

A - Click the menu items to open submenu links, and then click on a submenu link to open the screen in the main window.

B, **C**, **D**, **E** - These are quick links which allow you to perform certain tasks no matter which screen you are currently working in.

B - Click this link to save your configuration into the Switch's nonvolatile memory. Nonvolatile memory is the configuration of your Switch that stays the same even if the Switch's power is turned off.

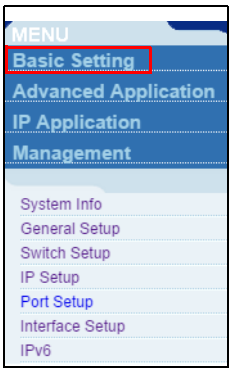
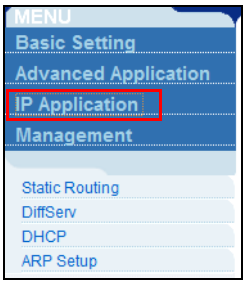
C - Click this link to go to the status page of the Switch.

D - Click this link to logout of the web configurator.

E - Click this link to display web help pages. The help pages provide descriptions for all of the configuration screens.

In the navigation panel, click a main link to reveal a list of submenu links.

Table 4 Navigation Panel Sub-links Overview

BASIC SETTING	ADVANCED APPLICATION	IP APPLICATION	MANAGEMENT
			

The following table describes the links in the navigation panel.

Table 5 Navigation Panel Links

LINK	DESCRIPTION
Basic Settings	
System Info	This link takes you to a screen that displays general system information.
General Setup	This link takes you to a screen where you can configure general identification information about the Switch.
Switch Setup	This link takes you to a screen where you can set up global Switch parameters such as VLAN type, GARP and priority queues.

Table 5 Navigation Panel Links (continued)

LINK	DESCRIPTION
IP Setup	This link takes you to a screen where you can configure the IP address, subnet mask (necessary for Switch management) and DNS (domain name server) and set up to 32 IP routing domains.
Port Setup	This link takes you to a screen where you can configure settings for individual Switch ports.
PoE Setup	For PoE model(s) This link takes you to a screen where you can set priorities so that the Switch is able to reserve and allocate power to certain PDs.
Interface Setup	This link takes you to a screen where you can configure settings for individual interface type and ID.
IPv6	This link takes you to a screen where you can view IPv6 status and configure IPv6 settings.
Advanced Application	
VLAN	This link takes you to screens where you can configure port-based or 802.1Q VLAN (depending on what you configured in the Switch Setup menu). You can also configure a protocol based VLAN or a subnet based VLAN in these screens.
Static MAC Forwarding	This link takes you to a screen where you can configure static MAC addresses for a port. These static MAC addresses do not age out.
Static Multicast Forwarding	This link takes you to a screen where you can configure static multicast MAC addresses for port(s). These static multicast MAC addresses do not age out.
Filtering	This link takes you to a screen to set up filtering rules.
Spanning Tree Protocol	This link takes you to screens where you can configure the RSTP/MRSTP/MSTP to prevent network loops.
Bandwidth Control	This link takes you to a screen where you can configure bandwidth limits on the Switch.
Broadcast Storm Control	This link takes you to a screen to set up broadcast filters.
Mirroring	This link takes you to screens where you can copy traffic from one port or ports to another port in order that you can examine the traffic from the first port without interference.
Link Aggregation	This link takes you to screens where you can logically aggregate physical links to form one logical, higher-bandwidth link.
Port Authentication	This link takes you to a screen where you can configure IEEE 802.1x port authentication for clients communicating via the Switch.
Port Security	This link takes you to screens where you can activate MAC address learning and set the maximum number of MAC addresses to learn on a port.
Time Range	This link takes you to a screen where you can configure time schedule profiles.
Classifier	This link takes you to a screen where you can configure the Switch to group packets based on the specified criteria.
Policy Rule	This link takes you to a screen where you can configure the Switch to perform special treatment on the grouped packets.
Queuing Method	This link takes you to a screen where you can configure queuing with associated queue weights for each port.
Multicast	This link takes you to screens where you can configure various multicast features, IGMP snooping and create multicast VLANs.
AAA	This link takes you to a screen where you can configure authentication, authorization services via external servers. The external servers can be either RADIUS (Remote Authentication Dial-In User Service) or TACACS+ (Terminal Access Controller Access-Control System Plus).
IP Source Guard	This link takes you to screens where you can configure filtering of unauthorized DHCP and ARP packets in your network.

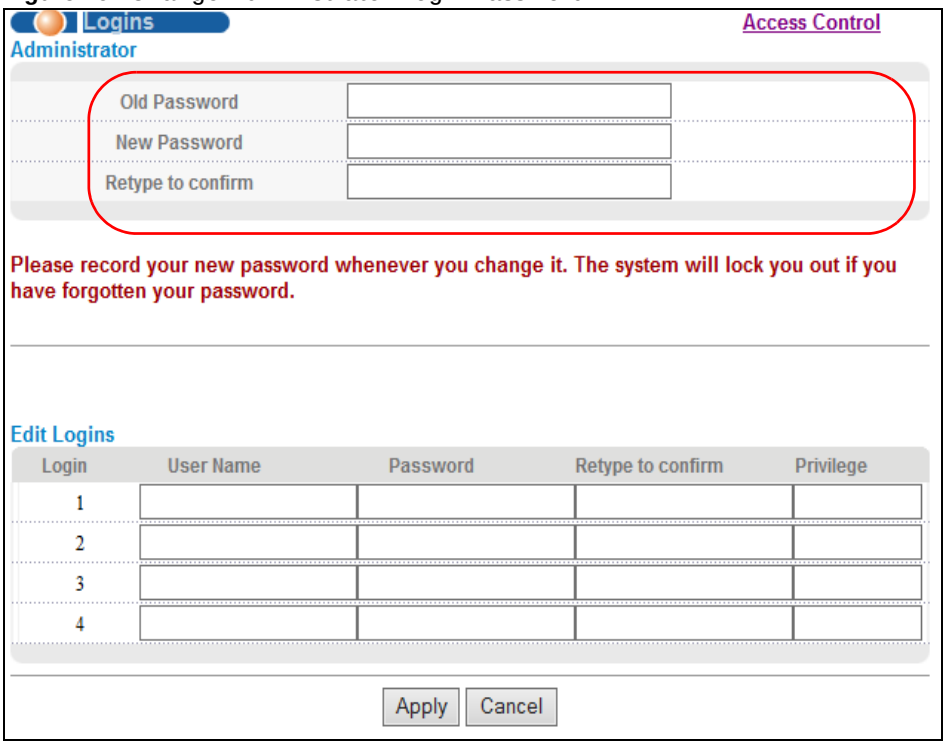
Table 5 Navigation Panel Links (continued)

LINK	DESCRIPTION
Loop Guard	This link takes you to a screen where you can configure protection against network loops that occur on the edge of your network.
Layer 2 Protocol Tunneling	This link takes you to a screen where you can configure L2PT (Layer 2 Protocol Tunneling) settings on the Switch.
PPPoE	This link takes you to a screen where you can configure intermediate agent settings in port, VLAN, and PPPoE.
Errdisable	This link takes you to a screen where you can configure errdisable settings in CPU protection, errdisable detect, and errdisable recovery.
MAC Pinning	This link takes you to a screen where you can configure MAC pinning. If you are connecting to multiple upstream switches that do not support port channels, then use MAC pinning to divide the uplinks into standalone links that pins the MAC addresses to those links in a round-robin method.
Private VLAN	This link takes you to a screen where you can configure private VLANs.
Green Ethernet	This link takes you to a screen where you can configure green Ethernet settings in EEE, auto power down, abd short reach for each port.
LLDP	This link takes you to a screen where you can configure LLDP settings.
IP Application	
Static Routing	This link takes you to a screen where you can configure static routes. A static route defines how the Switch should forward traffic by configuring the TCP/IP parameters manually.
DiffServ	This link takes you to screens where you can enable DiffServ, configure marking rules and set DSCP-to-IEEE802.1p mappings.
DHCP	This link takes you to screens where you can configure the DHCP settings.
ARP Setup	This link takes you to screens where you can configure the ARP learning settings for each port.
Management	
Maintenance	This link takes you to screens where you can perform firmware and configuration file maintenance as well as reboot the system.
Access Control	This link takes you to screens where you can change the system login password and configure SNMP and remote management.
Diagnostic	This link takes you to a screen where you can view system logs and test port(s).
Syslog	This link takes you to screens where you can setup system logs and a system log server.
Cluster Management	This link takes you to screens where you can configure clustering management and view its status.
MAC Table	This link takes you to a screen where you can view the MAC addresses (and types) of devices attached to what ports and VLAN IDs.
IP Table	This link takes you to a screen where you can view IP, VLAN ID and port information.
ARP Table	This link takes you to a screen where you can view the MAC addresses – IP address resolution table.
Routing Table	This link takes you to a screen where you can view the routing table containing, destination, gateway, interface, metric and type (static or dynamic) information.
Path MTU Table	This link takes you to a screen where you can view the path MTU aging time, index, destination address, MTU, and expire settings.
Configure Clone	This link takes you to a screen where you can copy attributes of one port to other ports.
Neighbor Table	This link takes you to a screen where you can view the IPv6 neighbor table which includes index, interface, neighbor address, MAC address, status and type.

4.3.1 Change Your Password

After you log in for the first time, it is recommended you change the default administrator password. Click **Management** > **Access Control** > **Logins** to display the next screen.

Figure 16 Change Administrator Login Password



4.4 Saving Your Configuration

When you are done modifying the settings in a screen, click **Apply** to save your changes back to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.

Click the **Save** link in the upper right hand corner of the web configurator to save your configuration to nonvolatile memory. Nonvolatile memory refers to the Switch's storage that remains even if the Switch's power is turned off.

Note: Use the **Save** link when you are done with a configuration session.

4.5 Switch Lockout

You could block yourself (and all others) from managing the Switch if you do one of the following:

1 Delete the management VLAN (default is VLAN 1).

2 Delete all port-based VLANs with the CPU port as a member. The “CPU port” is the management port of the Switch.

3 Filter all traffic to the CPU port.

4 Disable all ports.

5 Misconfigure the text configuration file.

6 Forget the password and/or IP address.

7 Prevent all services from accessing the Switch.

8 Change a service port number but forget it.

Note: Be careful not to lock yourself and others out of the Switch.

4.6 Resetting the Switch

If you lock yourself (and others) from the Switch or forget the administrator password, you will need to reset the Switch back to the factory defaults (see Section 3.4 on page 29).

4.7 Logging Out of the Web Configurator

Click **Logout** in a screen to exit the web configurator. You have to log in with your password again after you log out. This is recommended after you finish a management session for security reasons.

Figure 17 Web Configurator: Logout Screen

4.8 Help

The web configurator’s online help has descriptions of individual screens and some supplementary information.

Click the **Help** link from a web configurator screen to view an online help description of that screen.

5

Initial Setup Example

5.1 Overview

This chapter shows how to set up the Switch for an example network.

The following lists the configuration steps for the initial setup:

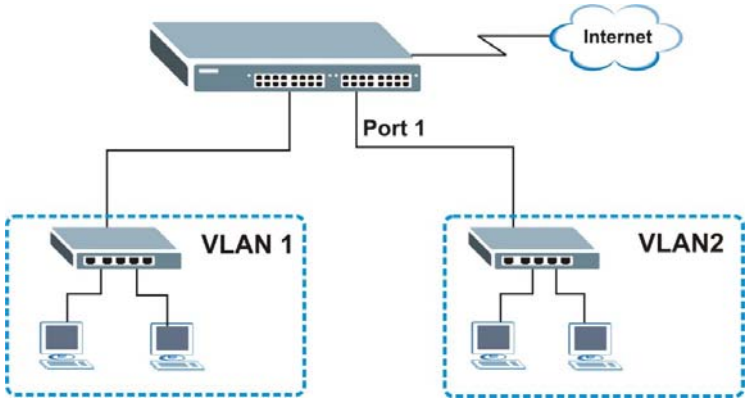
- Create a VLAN
- Set port VLAN ID
- Configure the Switch IP management address

5.1.1 Creating a VLAN

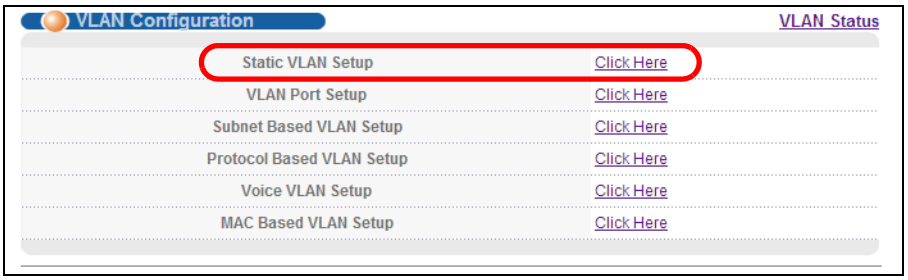
VLANs confine broadcast frames to the VLAN group in which the port(s) belongs. You can do this with port-based VLAN or tagged static VLAN with fixed port members.

In this example, you want to configure port 1 as a member of VLAN 2.

Figure 18 Initial Setup Network Example: VLAN



1 Click **Advanced Application** > **VLAN > VLAN Configuration** in the navigation panel and click the **Static VLAN Setup** link.



2 In the **Static VLAN** screen, select **ACTIVE**, enter a descriptive name in the **Name** field and enter 2 in the **VLAN Group ID** field for the **VLAN2** network.

Note: The **VLAN Group ID** field in this screen and the **VID** field in the **IP Setup** screen refer to the same VLAN ID.

3 Since the **VLAN2** network is connected to port 1 on the Switch, select **Fixed** to configure port 1 to be a permanent member of the VLAN only.

4 To ensure that VLAN-unaware devices (such as computers and hubs) can receive frames properly, clear the **TX Tagging** check box to set the Switch to remove VLAN tags before sending.

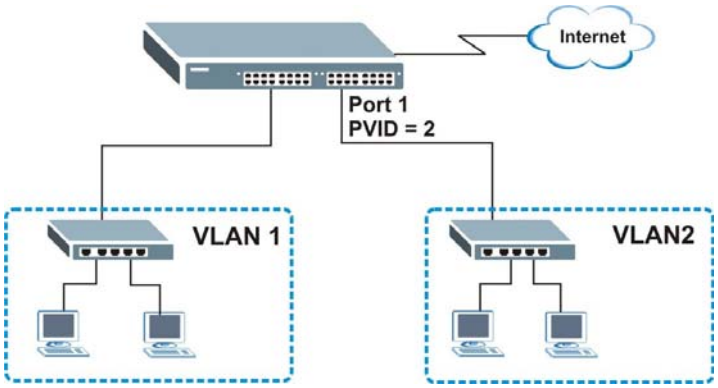
5 Click **Add** to save the settings to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.

5.1.2 Setting Port VID

Use PVID to add a tag to incoming untagged frames received on that port so that the frames are forwarded to the VLAN group that the tag defines.

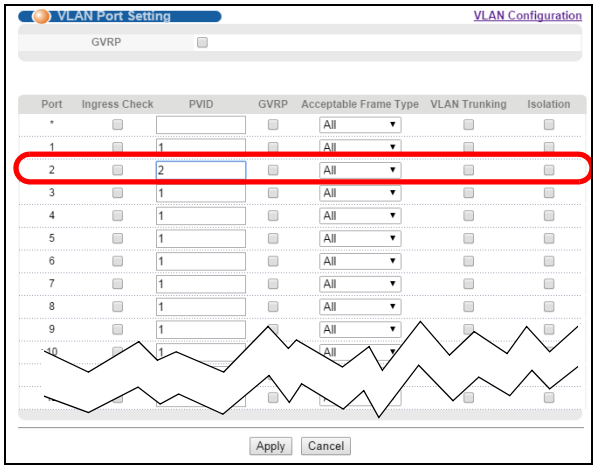
In the example network, configure 2 as the port VID on port 1 so that any untagged frames received on that port get sent to VLAN 2.

Figure 19 Initial Setup Network Example: Port VID



1 Click **Advanced Applications** > **VLAN** > **VLAN Configuration** in the navigation panel. Then click the **VLAN Port Setup** link.

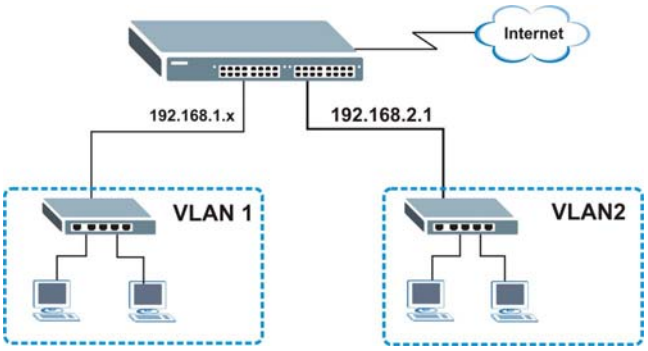
2 Enter 2 in the **PVID** field for port 2 and click **Apply** to save your changes back to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.



5.2 Configuring Switch Management IP Address

The default management IP address of the Switch is 192.168.1.1. You can configure another IP address in a different subnet for management purposes. The following figure shows an example.

Figure 20 Initial Setup Example: Management IP Address



1 Connect your computer to any Ethernet port on the Switch. Make sure your computer is in the same subnet as the Switch.

2 Open your web browser and enter 192.168.1.1 (the default IP address) in the address bar to access the web configurator. See Section 4.2 on page 32 for more information.

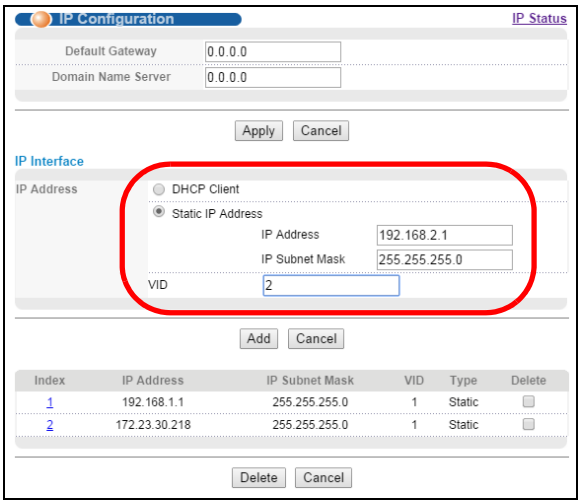
3 Click **Basic Setting** > **IP Setup** in the navigation panel.

4 Configure the related fields in the **IP Setup** screen.

5 For the **VLAN2** network, enter 192.168.2.1 as the IP address and 255.255.255.0 as the subnet mask.

6 In the **VID** field, enter the ID of the VLAN group to which you want this management IP address to belong. This is the same as the VLAN ID you configure in the **Static VLAN** screen.

7 Click **Add** to save your changes back to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.



6

Tutorials

6.1 Overview

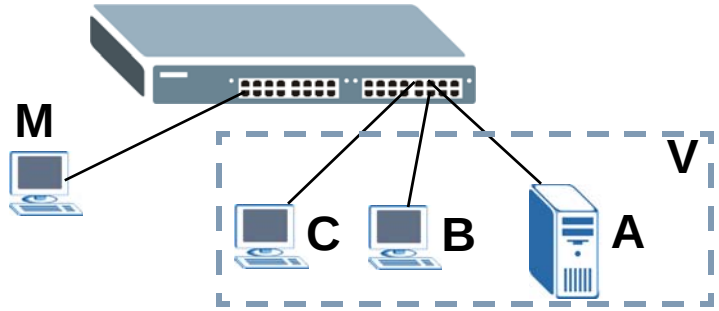
This chapter provides some examples of using the web configurator to set up and use the Switch. The tutorials include:

- How to Use DHCP Snooping on the Switch
- How to Use DHCP Relay on the Switch

6.2 How to Use DHCP Snooping on the Switch

You only want DHCP server **A** connected to port 5 to assign IP addresses to all devices in VLAN network (**V**). Create a VLAN containing ports 5, 6 and 7. Connect a computer **M** to the Switch for management.

Figure 21 Tutorial: DHCP Snooping Tutorial Overview



Note: For related information about DHCP snooping, see Section 26.1 on page 212.

The settings in this tutorial are as the following.

Table 6 Tutorial: Settings in this Tutorial

HOST	PORT CONNECTED	VLAN	PVID	DHCP SNOOPING PORT TRUSTED
DHCP Server (**A**)	5	1 and 100	100	Yes
DHCP Client (**B**)	6	1 and 100	100	No
DHCP Client (**C**)	7	1 and 100	100	No

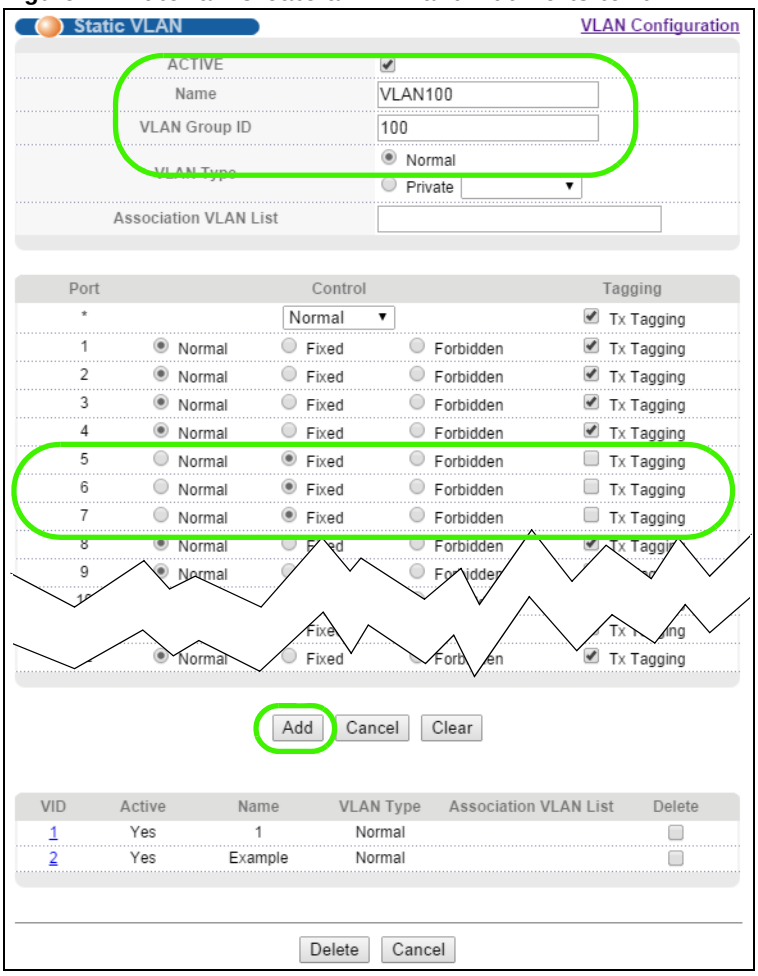
1 Access the Switch through **http://192.168.1.1** by default. Log into the Switch by entering the username (default: **admin**) and password (default: **1234**).

2 Go to **Advanced Application** > **VLAN** > **VLAN Configuration** > **Static VLAN Setup**, and create a VLAN with ID of 100. Add ports 5, 6 and 7 in the VLAN by selecting **Fixed** in the **Control** field as shown.

Deselect **Tx Tagging** because you don't want outgoing traffic to contain this VLAN tag.

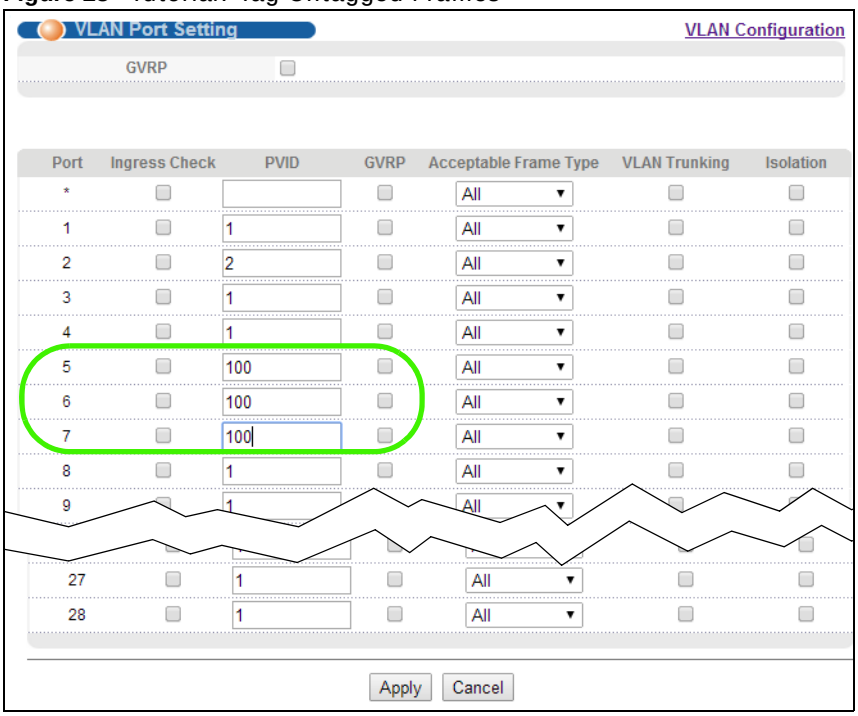
Click **Add**.

Figure 22 Tutorial: Create a VLAN and Add Ports to It



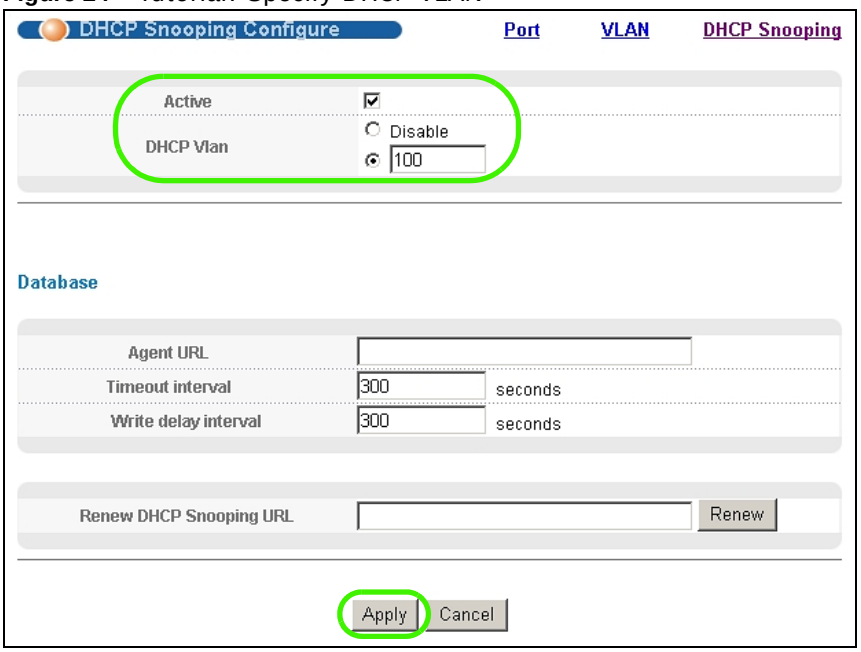
3 Go to **Advanced Application** > **VLAN** > **VLAN Configuration** > **VLAN Port Setup**, and set the PVID of the ports 5, 6 and 7 to 100. This tags untagged incoming frames on ports 5, 6 and 7 with the tag 100.

Figure 23 Tutorial: Tag Untagged Frames



4 Go to **Advanced Application** > **IP Source Guard** > **DHCP snooping** > **Configure**, activate and specify VLAN 100 as the DHCP VLAN as shown. Click **Apply**.

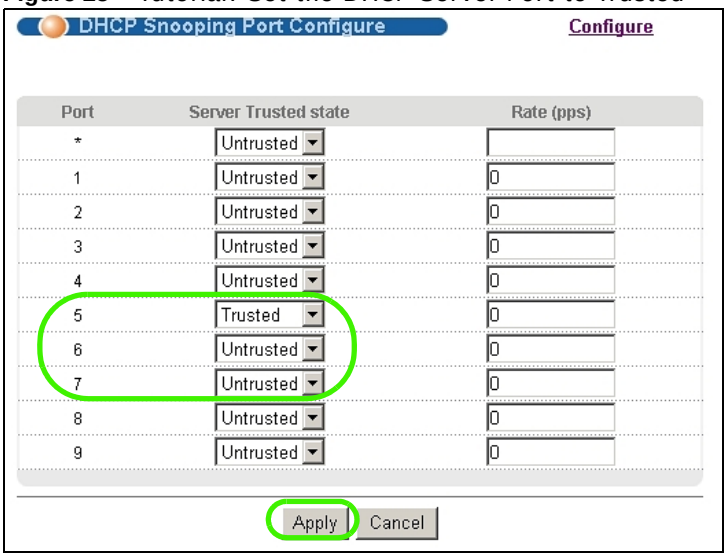
Figure 24 Tutorial: Specify DHCP VLAN



5 Click the **Port** link at the top right corner.

6 The **DHCP Snooping Port Configure** screen appears. Select **Trusted** in the **Server Trusted state** field for port 5 because the DHCP server is connected to port 5. Keep ports 6 and 7 **Untrusted** because they are connected to DHCP clients. Click **Apply**.

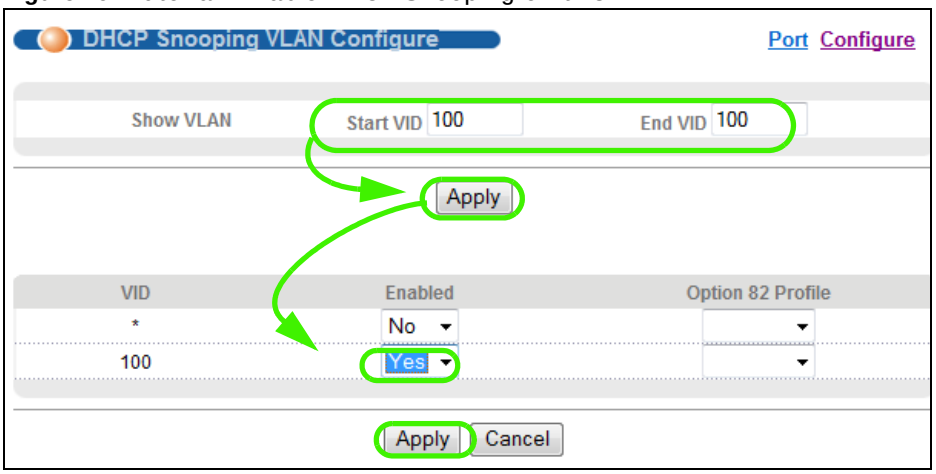
Figure 25 Tutorial: Set the DHCP Server Port to Trusted



7 Go to **Advanced Application** > **IP Source Guard** > **DHCP snooping** > **Configure** > **VLAN**, show VLAN 100 by entering 100 in the **Start VID** and **End VID** fields and click **Apply**. Then select **Yes** in the **Enabled** field of the VLAN 100 entry shown at the bottom section of the screen.

If you want to add more information in the DHCP request packets such as source VLAN ID or system name, you can also select the **Option82 Profile** field in the entry. See Section 26.10.1.3 on page 232.

Figure 26 Tutorial: Enable DHCP Snooping on this VLAN

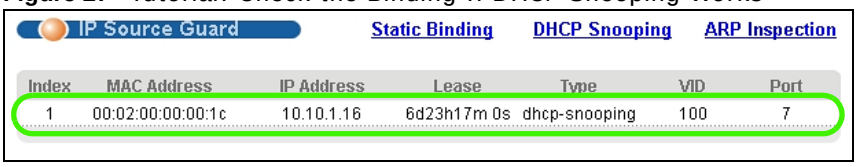


8 Click **Save** at the top right corner of the web configurator to save the configuration permanently.

9 Connect your DHCP server to port 5 and a computer (as DHCP client) to either port 6 or 7. The computer should be able to get an IP address from the DHCP server. If you put the DHCP server on port 6 or 7, the computer will not able to get an IP address.

10 To check if DHCP snooping works, go to **Advanced Application** > **IP Source Guard**, you should see an IP assignment with the type **DHCP-Snooping** as shown.

Figure 27 Tutorial: Check the Binding If DHCP Snooping Works



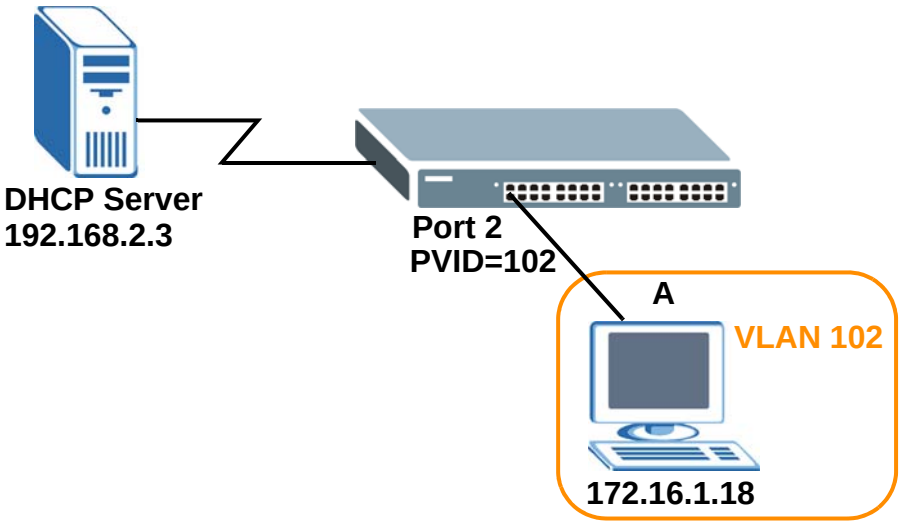
6.3 How to Use DHCP Relay on the Switch

This tutorial describes how to configure your Switch to forward DHCP client requests to a specific DHCP server. The DHCP server can then assign a specific IP address based on the information in the DHCP requests.

6.3.1 DHCP Relay Tutorial Introduction

In this example, you have configured your DHCP server (192.168.2.3) and want to have it assign a specific IP address (say 172.16.1.18) to DHCP client **A** based on the system name, VLAN ID and port number in the DHCP request. Client **A** connects to the Switch's port 2 in VLAN 102.

Figure 28 Tutorial: DHCP Relay Scenario

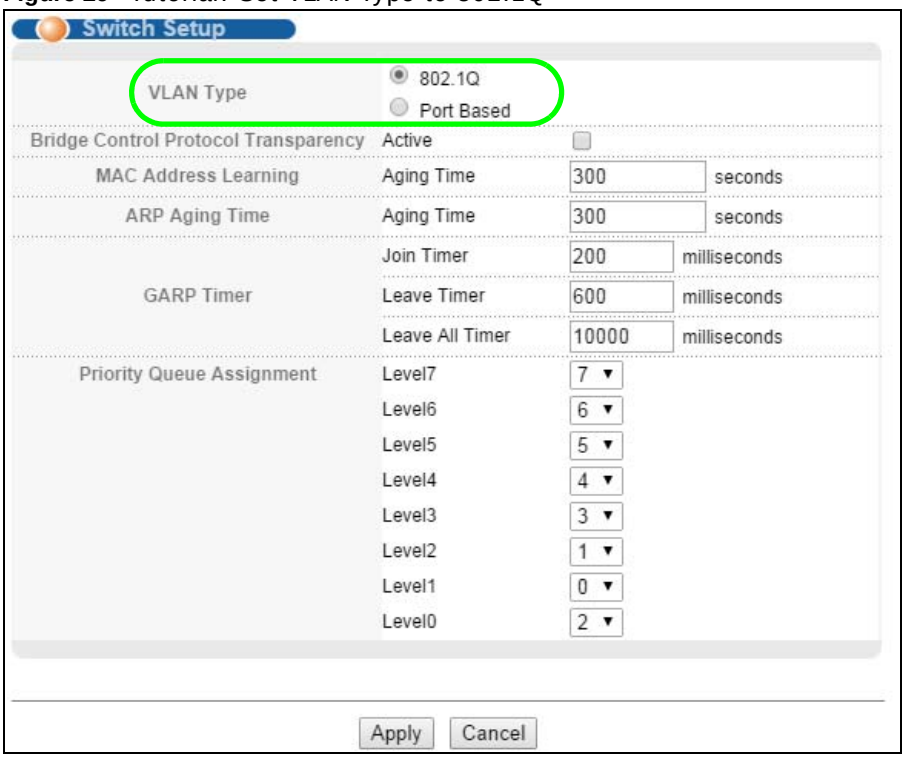


6.3.2 Creating a VLAN

Follow the steps below to configure port 2 as a member of VLAN 102.

1. Access the web configurator through the Switch's management port.
2. Go to **Basic Setting** > **Switch Setup** and set the VLAN type to **802.1Q**. Click **Apply** to save the settings to the run-time memory.

Figure 29 Tutorial: Set VLAN Type to 802.1Q



3 Click **Advanced Application** > **VLAN** > **VLAN Configuration** > **Static VLAN Setup**.

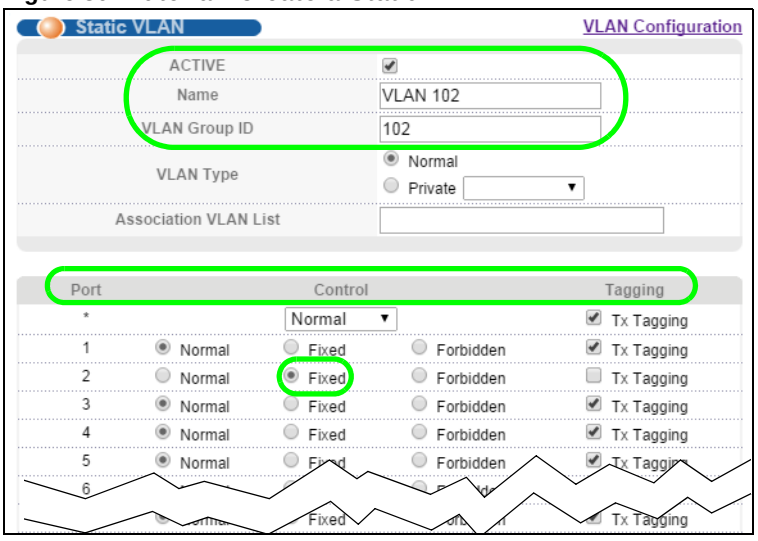
4 In the **Static VLAN** screen, select **ACTIVE**, enter a descriptive name (VLAN 102 for example) in the **Name** field and enter 102 in the **VLAN Group ID** field.

5 Select **Fixed** to configure port 2 to be a permanent member of this VLAN.

6 Clear the **TX Tagging** check box to set the Switch to remove VLAN tags before sending.

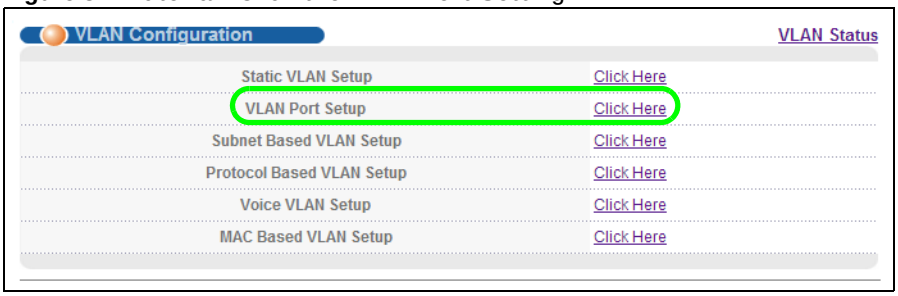
7 Click **Add** to save the settings to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.

Figure 30 Tutorial: Create a Static VLAN



8 Click the **VLAN Configuration** link in the **Static VLAN** screen and then the **VLAN Port Setup** link in the **VLAN Configuration** screen.

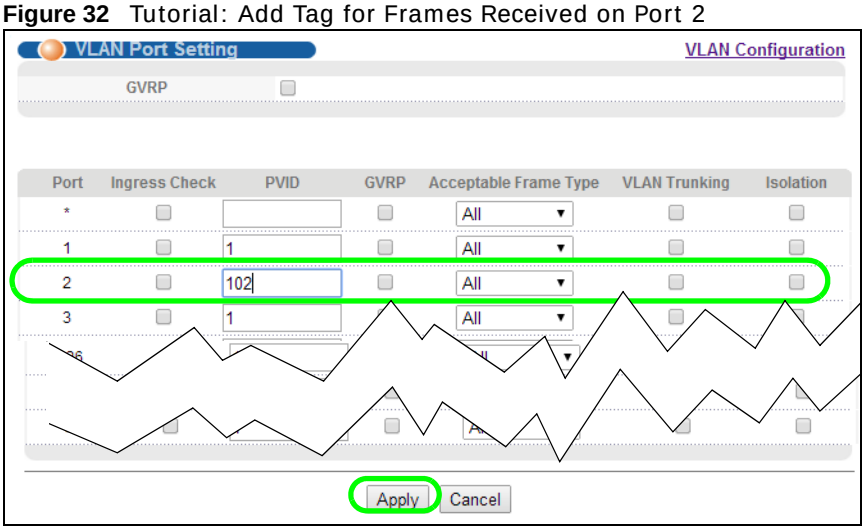
Figure 31 Tutorial: Click the VLAN Port Setting Link



9 Enter 102 in the **PVID** field for port 2 to add a tag to incoming untagged frames received on that port so that the frames are forwarded to the VLAN group that the tag defines.

10 Click **Apply** to save your changes back to the run-time memory.

Figure 32 Tutorial: Add Tag for Frames Received on Port 2



11 Click the **Save** link in the upper right corner of the web configurator to save your configuration permanently.

6.3.3 Configuring DHCP Relay

Follow the steps below to enable DHCP relay on the Switch and allow the Switch to add relay agent information (such as the VLAN ID) to DHCP requests.

1 Click **IP Application > DHCP > DHCPv4** and then the **Global** link to open the **DHCP Relay** screen.

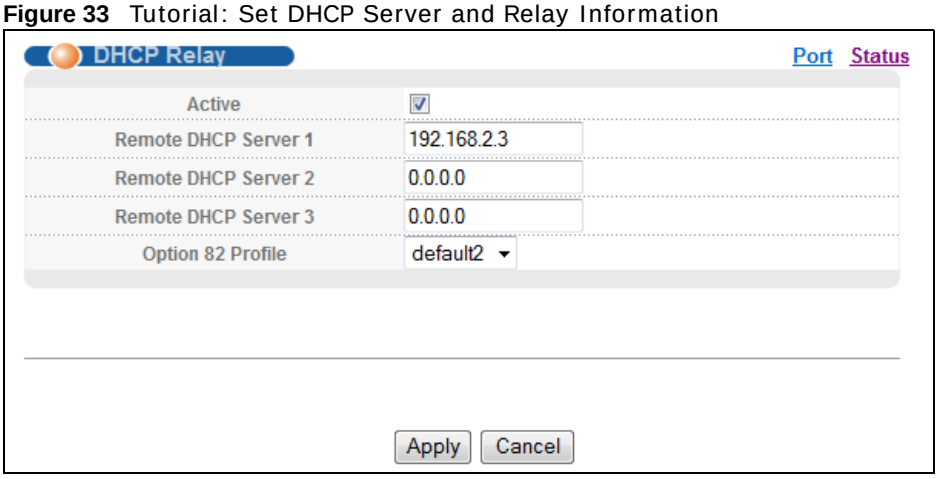
2 Select the **Active** check box.

3 Enter the DHCP server's IP address (192.168.2.3 in this example) in the **Remote DHCP Server 1** field.

4 Select **default1** or **default2** in the **Option 82 Profile** field.

5 Click **Apply** to save your changes back to the run-time memory.

Figure 33 Tutorial: Set DHCP Server and Relay Information



6 Click the **Save** link in the upper right corner of the web configurator to save your configuration permanently.

7 The DHCP server can then assign a specific IP address based on the DHCP request.

6.3.4 Troubleshooting

Check the client **A**'s IP address. If it did not receive the IP address 172.16.1.18, make sure:

1 Client **A** is connected to the Switch's port 2 in VLAN 102.

2 You configured the correct VLAN ID, port number and system name for DHCP relay on both the DHCP server and the Switch.

3 You clicked the **Save** link on the Switch to have your settings take effect.

7

ZON Utility, ZON Neighbor Management and Port Status

7.1 Overview

This chapter describes the screens for ZON Utility, ZON Neighbor Management, Port Status, Port Details and PoE status.

The home screen of the web configurator displays a port statistical summary with links to each port showing statistical details.

7.1.1 What You Can Do

- Use the **ZON Utility** screen (Section 7.2 on page 51) to deploy and manage network devices.
- Use **Neighbor** screen (Section 7.3 on page 52) to view and manage Switch's neighbor devices.
- Use the **Port Status Summary** screen (Section 7.4 on page 53) to view the port statistics.
- Use the **Port Details** screen (Section 7.4.1 on page 54) to display individual port statistics.

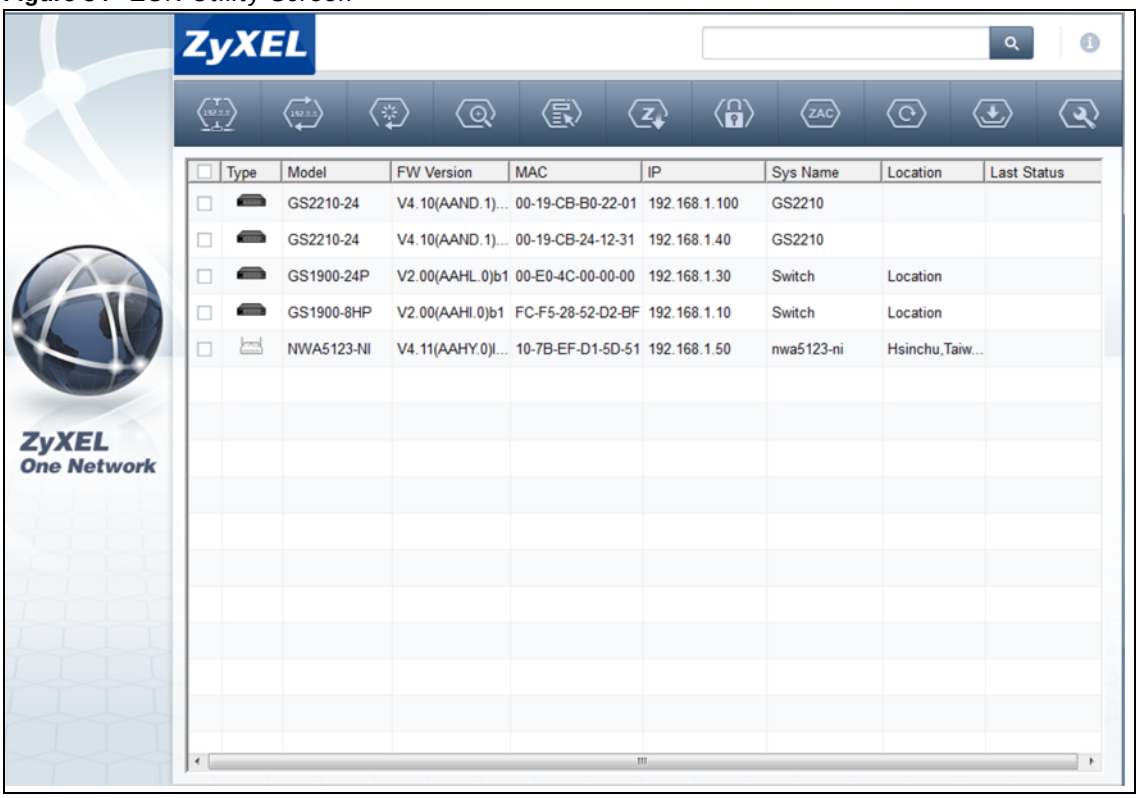
7.2 ZyXEL One Network (ZON) Utility Screen

ZON Utility is a program designed to help you deploy and manage a network more efficiently. It detects devices automatically and allows you to do basic settings on devices in the network without having to be near it.

The ZON Utility issues requests via ZyXEL Discovery Protocol (ZDP) and in response to the query, the device responds back with basic information including, IP address, firmware version, location, system and model name in the same broadcast domain. The information is then displayed in the ZON Utility screen and you can perform tasks like basic configuration of the devices and batch firmware upgrade in it. You can download the ZON Utility at www.zyxel.com and install it on a PC.

The following figure shows the ZON Utility screen.

Figure 34 ZON Utility Screen

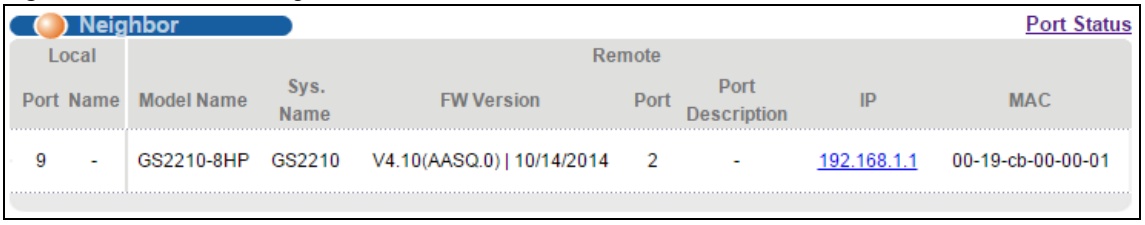


7.3 Neighbor Screen

The ZON Neighbor Management screen allows you to view and manage the Switch's neighboring devices more conveniently. It uses Layer Link Discovery Protocol (LLDP) to discover all neighbor devices connected to the Switch including non-ZyXEL devices. You can perform tasks on the neighboring devices like login, reboot (turn the power off and then back on again), and reset to factory default settings in the Neighbor Management screen. For more information on LLDP, see (Section 34.3 on page 268).

Click **Status** > **Neighbor** to see the following screen.

Figure 35 Status > Neighbor



The following table describes the fields in the above screen.

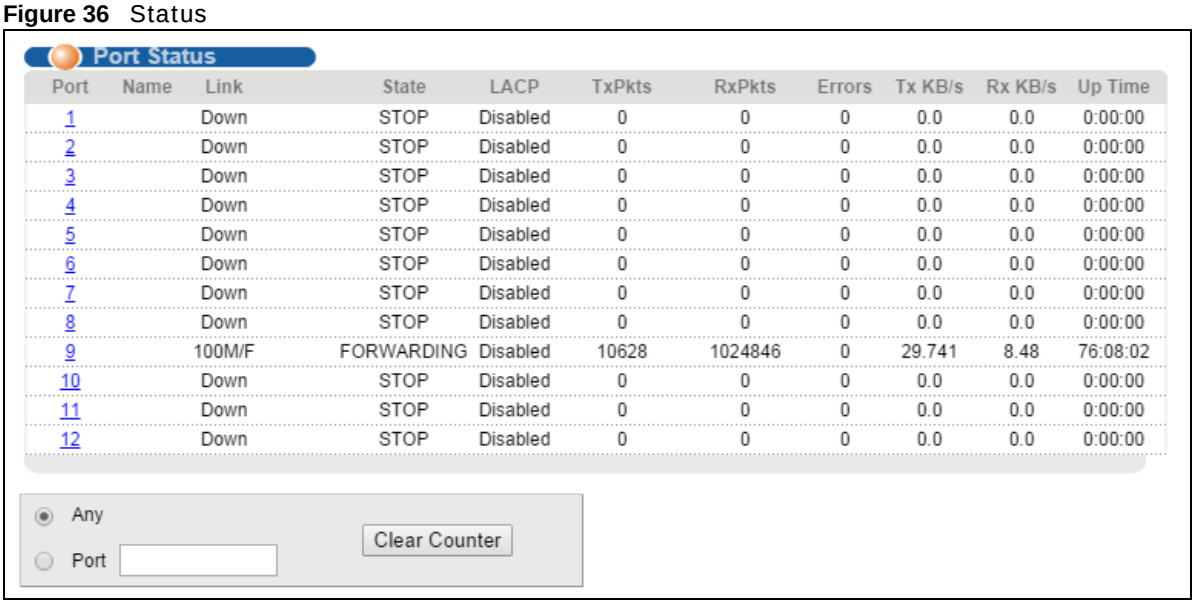
Table 7 Status > Neighbor

LABEL	DESCRIPTION
Local	
Port	This shows the port number of the local device in the network.
Name	This shows the name of the local device in the network.
Remote	
Model Name	This shows the model name of the neighbor device in the remote network. This field will show "**-**" for non-ZyXEL devices.
Sys. Name	This shows the system name of the neighbor device in the remote network.
FW Version	This shows the firmware version of the neighbor device in the remote network. This field will show "**-**" for non-ZyXEL devices.
Port	This show the port number of the neighbor device in the remote network.
Port Description	This shows the port description of the neighbor device in the remote network.
IP	This shows the IP address of the neighbor device in the remote network. The IP address is a **hyper link** that you can click and login the remote device. This field will show "**-**" for non-ZyXEL devices.
MAC	This shows the MAC address of the neighbor device in the remote network. This field will show "**-**" for non-ZyXEL devices.

7.4 Port Status Summary

To view the port statistics, click **Status** in all web configurator screens to display the **Status** screen as shown next.

Figure 36 Status


Port Status
Port Name Link State LACP TxPkts RxPkts Errors Tx KB/s Rx KB/s Up Time
1 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
2 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
3 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
4 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
5 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
6 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
7 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
8 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
9 100M/F FORWARDING Disabled 10628 1024846 0 29.741 8.48 76:08:02
10 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
11 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
12 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
Any
Port
Clear Counter

The following table describes the labels in this screen.

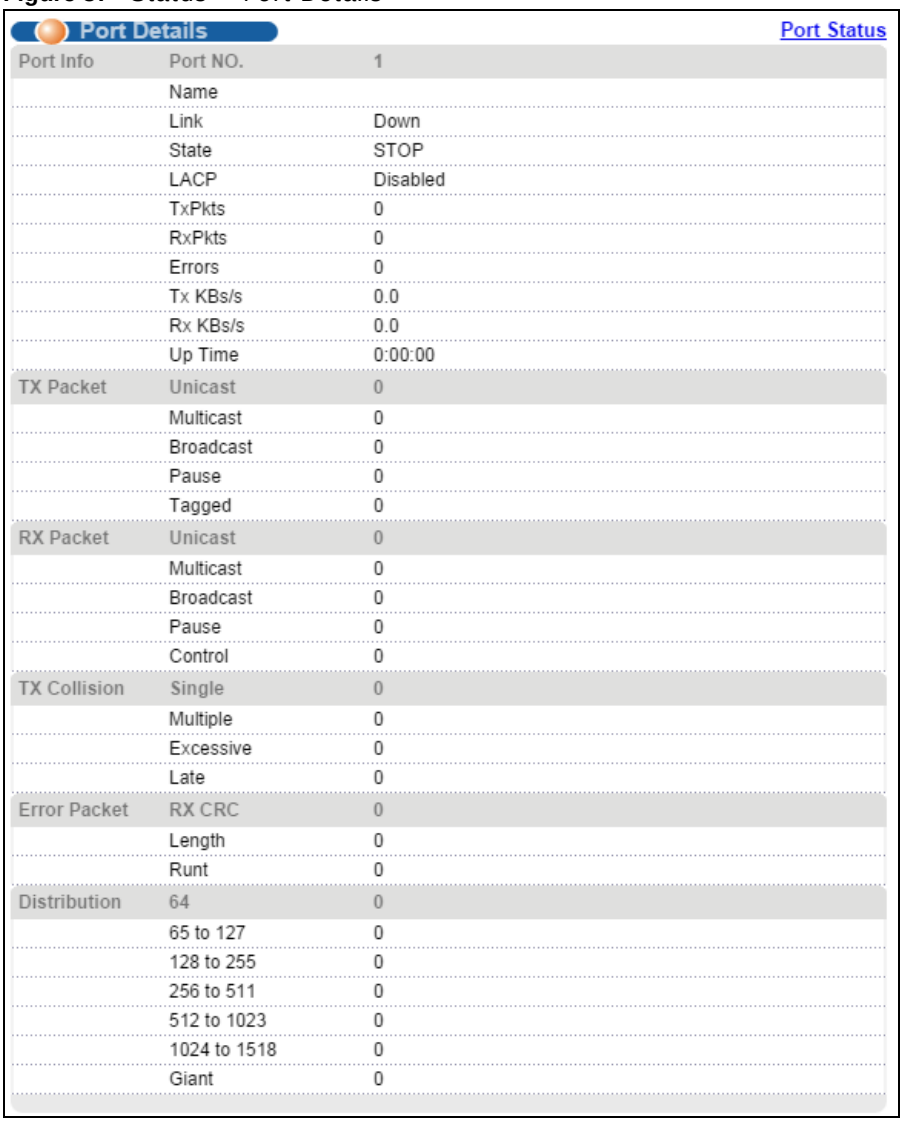
Table 8 Status

LABEL	DESCRIPTION
Port	This identifies the Ethernet port. Click a port number to display the **Port Details** screen (refer to Figure 37 on page 55).
Name	This is the name you assigned to this port in the **Basic Setting** > **Port Setup** screen.
Link	This field displays the speed (either **10M** for 10Mbps, **100M** for 100Mbps or **1000M** for 1000Mbps) and the duplex (**F** for full duplex or **H** for half). It also shows the cable type (**Copper** or **Fiber**) for the combo ports.
State	If STP (Spanning Tree Protocol) is enabled, this field displays the STP state of the port. See (Section 13.1 on page 115) for more information. If STP is disabled, this field displays **FORWARDING** if the link is up, otherwise, it displays **STOP**.
LACP	This fields displays whether LACP (Link Aggregation Control Protocol) has been enabled on the port.
TxPkts	This field shows the number of transmitted frames on this port.
RxPkts	This field shows the number of received frames on this port.
Errors	This field shows the number of received errors on this port.
Tx KB/s	This field shows the number of kilobytes per second transmitted on this port.
Rx KB/s	This field shows the number of kilobytes per second received on this port.
Up Time	This field shows the total amount of time in hours, minutes and seconds the port has been up.
Clear Counter	Enter a port number and then click **Clear Counter** to erase the recorded statistical information for that port, or select **Any** to clear statistics for all ports.

7.4.1 Status: Port Details

Click a number in the **Port** column in the **Status** screen to display individual port statistics. Use this screen to check status and detailed performance data about an individual port on the Switch.

Figure 37 Status > Port Details



The following table describes the labels in this screen.

Table 9 Status: Port Details

LABEL	DESCRIPTION
Port Info	
Port NO.	This field displays the port number you are viewing.
Name	This field displays the name of the port.
Link	This field displays the speed (either **10M** for 10Mbps, **100M** for 100Mbps or **1000M** for 1000Mbps) and the duplex (**F** for full duplex or **H** for half duplex). It also shows the cable type (**Copper** or **Fiber**).
Status	If STP (Spanning Tree Protocol) is enabled, this field displays the STP state of the port (see Section 13.1 on page 115 for more information). If STP is disabled, this field displays **FORWARDING** if the link is up, otherwise, it displays **STOP**.
LACP	This field shows if LACP is enabled on this port or not.
TxPkts	This field shows the number of transmitted frames on this port

Table 9 Status: Port Details (continued)

LABEL	DESCRIPTION
RxPkts	This field shows the number of received frames on this port
Errors	This field shows the number of received errors on this port.
Tx KB/s	This field shows the number of kilobytes per second transmitted on this port.
Rx KB/s	This field shows the number of kilobytes per second received on this port.
Up Time	This field shows the total amount of time the connection has been up.
Tx Packet The following fields display detailed information about packets transmitted.	
Unicast	This field shows the number of good unicast packets transmitted.
Multicast	This field shows the number of good multicast packets transmitted.
Broadcast	This field shows the number of good broadcast packets transmitted.
Pause	This field shows the number of 802.3x Pause packets transmitted.
Tagged	This field shows the number of VLAN tagged packets transmitted.
Rx Packet The following fields display detailed information about packets received.	
Unicast	This field shows the number of good unicast packets received.
Multicast	This field shows the number of good multicast packets received.
Broadcast	This field shows the number of good broadcast packets received.
Pause	This field shows the number of 802.3x Pause packets received.
Control	This field shows the number of control packets received (including those with CRC errors) but does not include 802.3x Pause packetss.
TX Collision The following fields display information on collisions while transmitting.	
Single	This is a count of successfully transmitted packets for which transmission is inhibited by exactly one collision.
Multiple	This is a count of successfully transmitted packets for which transmission was inhibited by more than one collision.
Excessive	This is a count of packets for which transmission failed due to excessive collisions. Excessive collision is defined as the number of maximum collisions before the retransmission count is reset.
Late	This is the number of times a late collision is detected, that is, after 512 bits of the packets have already been transmitted.
Error Packet	The following fields display detailed information about packets received that were in error.
RX CRC	This field shows the number of packets received with CRC (Cyclic Redundant Check) error(s).
Length	This field shows the number of packets received with a length that was out of range.
Runt	This field shows the number of packets received that were too short (shorter than 64 octets), including the ones with CRC errors.
Distribution	
64	This field shows the number of packets (including bad packets) received that were 64 octets in length.
65-127	This field shows the number of packets (including bad packets) received that were between 65 and 127 octets in length.
128-255	This field shows the number of packets (including bad packets) received that were between 128 and 255 octets in length.

Table 9 Status: Port Details (continued)

LABEL	DESCRIPTION
256-511	This field shows the number of packets (including bad packets) received that were between 256 and 511 octets in length.
512-1023	This field shows the number of packets (including bad packets) received that were between 512 and 1023 octets in length.
1024-1518	This field shows the number of packets (including bad packets) received that were between 1024 and 1518 octets in length.
Giant	This field shows the number of packets (including bad packets) received that were between 1519 octets and the maximum frame size. The maximum frame size varies depending on your switch model.

8

Basic Setting

8.1 Overview

This chapter describes how to configure the **System Info, General Setup**, **Switch Setup**, **IP Setup**, **Port Setup**, **PoE, Interface Setup** and **IPv6** screens.

8.1.1 What You Can Do

- Use the **System Info** screen (Section 8.8 on page 71) to check the firmware version number.
- Use the **General Setup** screen (Section 8.3 on page 60) to configure general settings such as the system name and time.
- Use the **Switch Setup** screen (Section 8.5 on page 63) to choose your VLAN type, set the GARP timers and assign priorities to queues.
- Use the **IP Setup** screen (Section on page 65) to configure the Switch IP address, default gateway device, the default domain name server and the management VLAN ID.
- Use the **Port Setup** screen (Section 8.7 on page 69) to configure Switch port settings.
-
- Use the **Interface Setup** screens (Section 8.8 on page 71) to configure Switch interface type and interface ID settings.
- Use the **IPv6** screens (Section 8.8 on page 71) to view IPv6 status and IPv6 configuration.

8.2 System Information

In the navigation panel, click **Basic Setting** > **System Info** to display the screen as shown. You can check the firmware version number.

Figure 38 Basic Setting > System Info

System Info

System Name	XS1920
Product Model	XS1920-12
ZyNOS F/W Version	V4.20(AASR.0)b4 | 08/26/2014
Ethernet Address	00:19:cb:00:00:01

CPU Utilization

Current (%)	16.21

Memory Utilization

Name	Total (byte)	Used (byte)	Utilization (%)
common	17104000	5624000	32

Hardware Monitor

Temperature Unit C

Temperature (C)	Current	MAX	MIN	Threshold	Status
MAC	51.0	54.0	44.0	90.0	Normal
CPU	52.0	55.0	46.0	90.0	Normal
PHY_1	56.0	59.0	47.0	92.0	Normal
PHY_2	55.0	58.0	47.0	92.0	Normal
BOARD	44.0	47.0	38.0	70.0	Normal
PHY_3	52.0	56.0	46.0	92.0	Normal
PHY_4	53.0	56.0	46.0	92.0	Normal
PHY_5	53.0	57.0	45.0	92.0	Normal
FAN Speed (RPM)	**Current**	**MAX**	**MIN**	**Threshold**	**Status**
FAN1	4560	9473	3673	500	Normal
FAN2	4683	9574	3744	500	Normal
FAN3	4757	9944	3776	500	Normal
Voltage (V)	**Current**	**MAX**	**MIN**	**Threshold**	**Status**
1.0V_MAC	1.009	1.009	1.009	+/-6%	Normal
1.0V	1.009	1.009	1.009	+/-6%	Normal
0.85V	0.852	0.852	0.852	+/-6%	Normal
1.5V	1.503	1.503	1.503	+/-5%	Normal
1.0V_AVS	1.013	1.013	1.013	+/-6%	Normal
1.8V	1.798	1.798	1.798	+/-6%	Normal
0.75V	0.755	0.755	0.744	+/-6%	Normal
3.3V	3.291	3.291	3.291	+/-6%	Normal
2.5V	2.513	2.539	2.513	+/-6%	Normal
12V	12.281	12.281	12.218	+/-10%	Normal

The following table describes the labels in this screen.

Table 10 Basic Setting > System Info

LABEL	DESCRIPTION
System Name	This field displays the descriptive name of the Switch for identification purposes.
Product Model	This field displays the product model of the Switch. Use this information when searching for firmware upgrade or looking for other support information in the website.
ZyNOS F/W Version	This field displays the version number of the Switch 's current firmware including the date created.
Ethernet Address	This field refers to the Ethernet MAC (Media Access Control) address of the Switch.
CPU Utilization	CPU utilization quantifies how busy the system is. **Current (%)** displays the current percentage of CPU utilization.
Memory Utilization	Memory Utilization shows how much DRAM memory is available and in use. It also displays the current percentage of memory utilization.
Name	This field displays the name of memory pool.

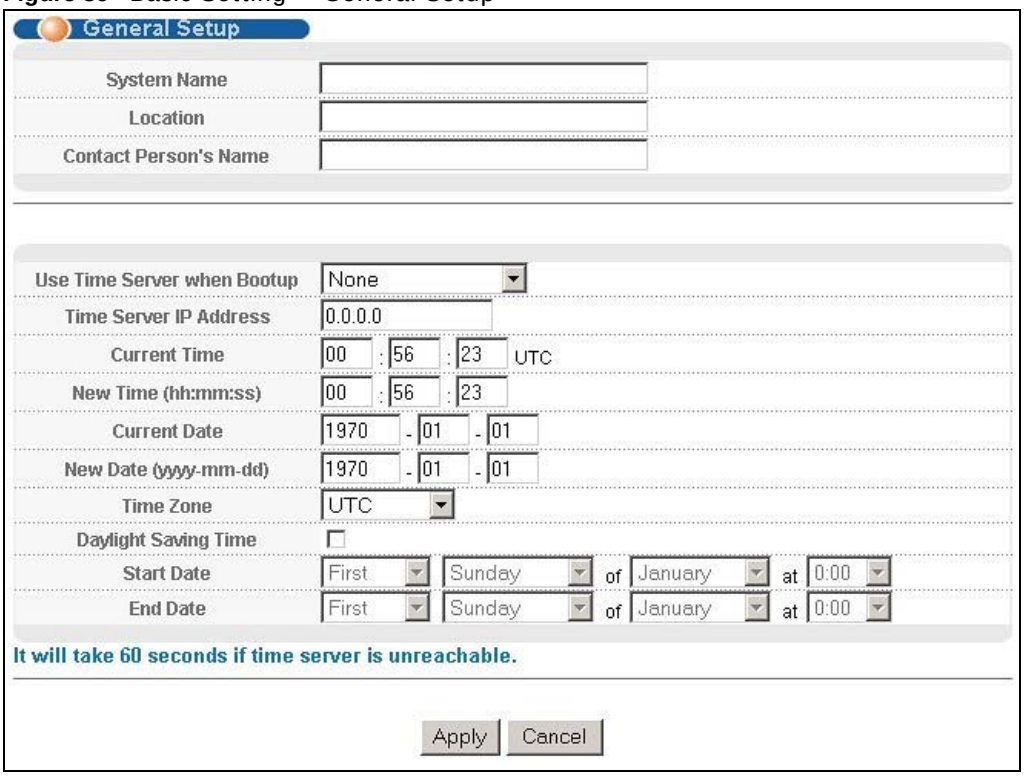
Table 10 Basic Setting > System Info (continued)

LABEL	DESCRIPTION
Total	This field displays the total number of bytes in this memory pool.
Used	This field displays the number of bytes being used in this memory pool.
Utilization	This field displays the percentage (%) of memory being used in this memory pool.
Hardware Monitor	
Temperature Unit	The Switch has temperature sensors that are capable of detecting and reporting if the temperature rises above the threshold. You may choose the temperature unit (Centigrade or Fahrenheit) in this field.
Temperature	**BOARD**, **MAC** and **PHY** refer to the location of the temperature sensors on the Switch printed circuit board.
Current	This shows the current temperature at this sensor.
MAX	This field displays the maximum temperature measured at this sensor.
MIN	This field displays the minimum temperature measured at this sensor.
Threshold	This field displays the upper temperature limit at this sensor.
Status	This field displays **Normal** for temperatures below the threshold and **Error** for those above.
Fan Speed (RPM)	A properly functioning fan is an essential component (along with a sufficiently ventilated, cool operating environment) in order for the device to stay within the temperature threshold. Each fan has a sensor that is capable of detecting and reporting if the fan speed falls below the threshold shown.
Current	This field displays this fan's current speed in Revolutions Per Minute (RPM).
MAX	This field displays this fan's maximum speed measured in Revolutions Per Minute (RPM).
MIN	This field displays this fan's minimum speed measured in Revolutions Per Minute (RPM). "<41" is displayed for speeds too small to measure (under 2000 RPM).
Threshold	This field displays the minimum speed at which a normal fan should work.
Status	**Normal** indicates that this fan is functioning above the minimum speed. **Error** indicates that this fan is functioning below the minimum speed.
Voltage(V)	The power supply for each voltage has a sensor that is capable of detecting and reporting if the voltage falls out of the tolerance range.
Current	This is the current voltage reading.
MAX	This field displays the maximum voltage measured at this point.
MIN	This field displays the minimum voltage measured at this point.
Threshold	This field displays the percentage tolerance of the voltage with which the Switch still works.
Status	**Normal** indicates that the voltage is within an acceptable operating range at this point; otherwise **Error** is displayed.

8.3 General Setup

Use this screen to configure general settings such as the system name and time. Click **Basic Setting** > **General Setup** in the navigation panel to display the screen as shown.

Figure 39 Basic Setting > General Setup



The following table describes the labels in this screen.

Table 11 Basic Setting > General Setup

LABEL	DESCRIPTION
System Name	Choose a descriptive name for identification purposes. This name consists of up to 64 printable characters; spaces are allowed.
Location	Enter the geographic location of your Switch. You can use up to 32 printable ASCII characters; spaces are allowed.
Contact Person's Name	Enter the name of the person in charge of this Switch. You can use up to 32 printable ASCII characters; spaces are allowed.
Use Time Server when Bootup	Enter the time service protocol that your timeserver uses. Not all time servers support all protocols, so you may have to use trial and error to find a protocol that works. The main differences between them are the time format. When you select the **Daytime (RFC 867)** format, the Switch displays the day, month, year and time with no time zone adjustment. When you use this format it is recommended that you use a Daytime timeserver within your geographical time zone. **Time (RFC-868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. **NTP (RFC-1305)** is similar to **Time (RFC-868)**. **None** is the default value. Enter the time manually. Each time you turn on the Switch, the time and date will be reset to 1970-1-1 0:0:0.
Time Server IP Address	Enter the IP address of your timeserver. The Switch searches for the timeserver for up to 60 seconds. If you select a timeserver that is unreachable, then this screen will appear locked for 60 seconds. Please wait.
Current Time	This field displays the time you open this menu (or refresh the menu).

Table 11 Basic Setting > General Setup (continued)

LABEL	DESCRIPTION
New Time (hh:min:ss)	Enter the new time in hour, minute and second format. The new time then appears in the **Current Time** field after you click **Apply**.
Current Date	This field displays the date you open this menu.
New Date (yyyy-mm-dd)	Enter the new date in year, month and day format. The new date then appears in the **Current Date** field after you click **Apply**.
Time Zone	Select the time difference between UTC (Universal Time Coordinated, formerly known as GMT, Greenwich Mean Time) and your time zone from the drop-down list box.
Daylight Saving Time	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected **Daylight Saving Time**. The time is displayed in the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Second**, **Sunday**, **March** and **2:00**. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **March** and the last field depends on your time zone. In Germany for instance, you would select **2:00** because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you selected **Daylight Saving Time**. The time field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **November** and **2:00**. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **October** and the last field depends on your time zone. In Germany for instance, you would select **2:00** because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

8.4 Introduction to VLANs

A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.

In MTU (Multi-Tenant Unit) applications, VLAN is vital in providing isolation and security among the subscribers. When properly configured, VLAN prevents one subscriber from accessing the network resources of another on the same LAN, thus a user will not see the printers and hard disks of another user in the same building.

VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

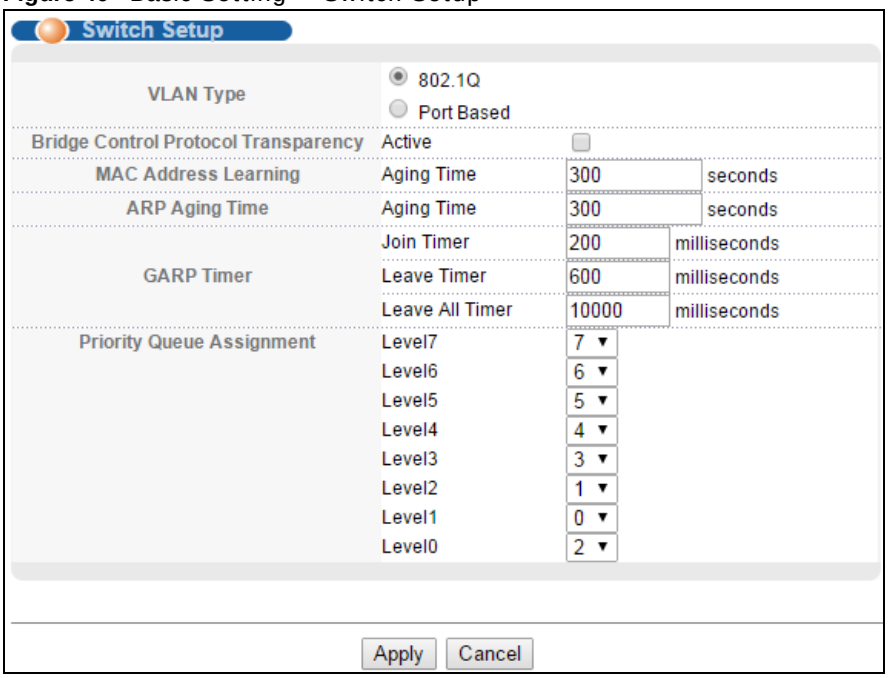
Note: VLAN is unidirectional; it only governs outgoing traffic.

See Chapter 9 on page 86 for information on port-based and 802.1Q tagged VLANs.

8.5 Switch Setup Screen

Click **Basic Setting** > **Switch Setup** in the navigation panel to display the screen as shown. The VLAN setup screens change depending on whether you choose **802.1Q** or **Port Based** in the **VLAN Type** field in this screen. Refer to Chapter 9 on page 86 for more information on VLAN.

Figure 40 Basic Setting > Switch Setup



The following table describes the labels in this screen.

Table 12 Basic Setting > Switch Setup

LABEL	DESCRIPTION
VLAN Type	Choose **802.1Q** or **Port Based**. The **VLAN Setup** screen changes depending on whether you choose **802.1Q** VLAN type or **Port Based** VLAN type in this screen. See Chapter 9 on page 86 for more information.
Bridge Control Protocol Transparency	Select **Active** to allow the Switch to handle bridging control protocols (STP, for example). You also need to define how to treat a BPDU in the **Port Setup** screen.
MAC Address Learning	MAC address learning reduces outgoing traffic broadcasts. For MAC address learning to occur on a port, the port must be active.
Aging Time	Enter a time from 10 to 1000000 seconds. This is how long all dynamically learned MAC addresses remain in the MAC address table before they age out (and must be relearned).

Table 12 Basic Setting > Switch Setup (continued)

LABEL	DESCRIPTION
ARP Aging Time	
Aging Time	Enter a time from 60 to 1000000 seconds. This is how long dynamically learned ARP entries remain in the ARP table before they age out (and must be relearned). The setting here applies to ARP entries which are newly added in the ARP table after you click **Apply**.
GARP Timer: Switches join VLANs by making a declaration. A declaration is made by issuing a **Join** message using GARP. Declarations are withdrawn by issuing a **Leave** message. A **Leave All** message terminates all registrations. GARP timers set declaration timeout values. See the chapter on VLAN setup for more background information.	
Join Timer	Join Timer sets the duration of the Join Period timer for GVRP in milliseconds. Each port has a **Join Period** timer. The allowed **Join Time** range is between 100 and 65535 milliseconds; the default is 200 milliseconds. See the chapter on VLAN setup for more background information.
Leave Timer	Leave Time sets the duration of the **Leave Period** timer for GVRP in milliseconds. Each port has a single **Leave Period** timer. Leave Time must be two times larger than **Join Timer**; the default is 600 milliseconds.
Leave All Timer	Leave All Timer sets the duration of the Leave All Period timer for GVRP in milliseconds. Each port has a single Leave All Period timer. Leave All Timer must be larger than Leave Timer.
Priority Queue Assignment IEEE 802.1p defines up to eight separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Frames without an explicit priority tag are given the default priority of the ingress port. Use the next fields to configure the priority level-to-physical queue mapping. The Switch has eight physical queues that you can map to the 8 priority levels. On the Switch, traffic assigned to higher index queues gets through faster while traffic in lower index queues is dropped if the network is congested.	
Priority Level (The following descriptions are based on the traffic types defined in the IEEE 802.1d standard (which incorporates the 802.1p).	
Level 7	Typically used for network control traffic such as router configuration messages.
Level 6	Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).
Level 5	Typically used for video that consumes high bandwidth and is sensitive to jitter.
Level 4	Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.
Level 3	Typically used for “excellent effort” or better than best effort and would include important business traffic that can tolerate some delay.
Level 2	This is for “spare bandwidth”.
Level 1	This is typically used for non-critical “background” traffic such as bulk transfers that are allowed but that should not affect other applications and users.
Level 0	Typically used for best-effort traffic.
Apply	Click **Apply** to save your changes to the Switch’s run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields.

8.6 IP Setup

Use the **IP Setup** screens to configure the Switch IP address, default gateway device, the default domain name server and the management VLAN ID. The default gateway specifies the IP address of the default gateway (next hop) for outgoing traffic.

The Switch needs an IP address for it to be managed over the network. The factory default IP address is 192.168.1.1. The subnet mask specifies the network number portion of an IP address. The factory default subnet mask is 255.255.255.0.

You can configure up to 32 IP addresses which are used to access and manage the Switch from the ports belonging to the pre-defined VLAN(s).

Note: You must configure a VLAN first.

8.6.1 IP Status

Use this screen to view configured IP settings as shown

Figure 41 Basic Setting > IP Status

The following table describes the labels in this screen.

Table 13 Basic Setting > IP Status

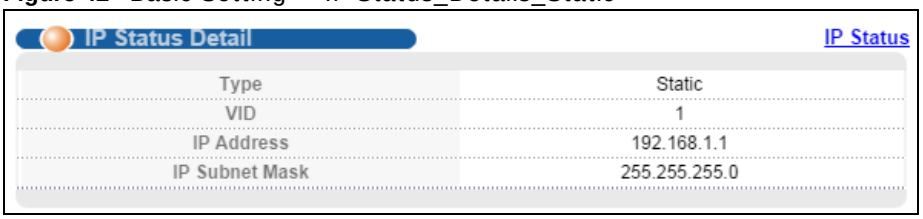
LABEL	DESCRIPTION
Index	Click the index link to view further details on this IP address.
IP Address	This is the IP address of your Switch in dotted decimal notation for example 192.168.1.1.
IP Subnet Mask	This is the IP subnet mask of your Switch in dotted decimal notation for example 255.255.255.0.
VID	This is thehe VLAN identification number to which an IP routing domain belongs..
Type	This shows whether ths IP address is dynamically assigned from a DHCP server or manually assigned (**Static**).
Renew	Click this to renew the dynamic IP address.
Release	Click this to release the dynamic IP address.

8.6.2 IP Status Details

Click the index link in the **IP Status** screen to view further details on this IP address.

Static IP Details

Figure 42 Basic Setting > IP Status_Details_Static



The following table describes the labels in this screen.

Table 14 Basic Setting > IP Status_Static

LABEL	DESCRIPTION
Type	This shows whether ths IP address is dynamically assigned from a DHCP server or manually assigned (**Static** or DHCP).
VID	This is the VLAN identification number to which an IP routing domain belongs.
IP Address	This is the IP address of your Switch in dotted decimal notation for example 192.168.1.1.
IP Subnet Mask	This is the IP subnet mask of your Switch in dotted decimal notation for example 255.255.255.0.

Dynamic IP Details (DHCP)

Figure 43 DHCP Lease Time

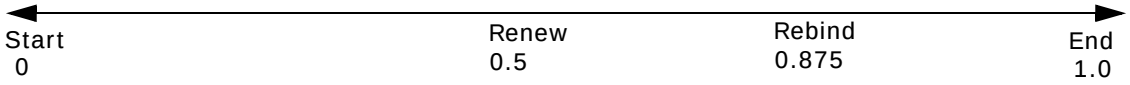
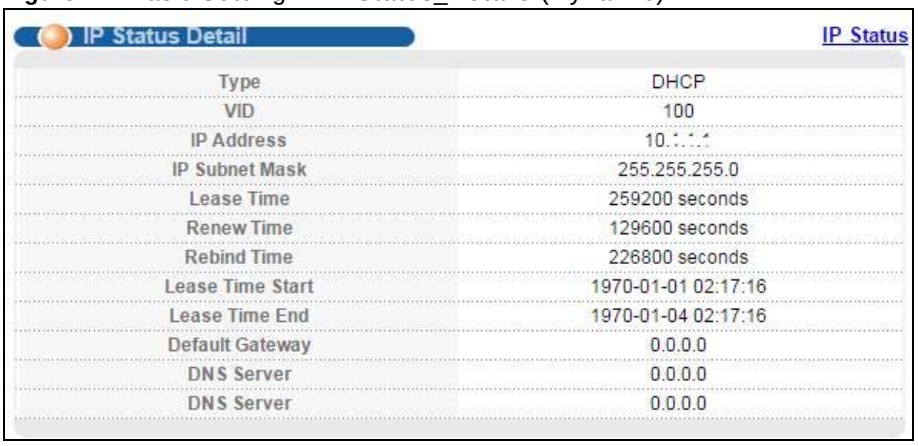


Figure 44 Basic Setting > IP Status_Details (Dynamic)



The following table describes the labels in this screen.

Table 15 Basic Setting > IP Status_Details (Dynamic)

LABEL	DESCRIPTION
Type	This shows whether ths IP address is dynamically assigned from a DHCP server or manually assigned (Static or **DHCP**).
VID	This is the VLAN identification number to which an IP routing domain belongs.
IP Address	This is the IP address of your Switch in dotted decimal notation for example 192.168.1.1.

Table 15 Basic Setting > IP Status_Details (Dynamic) (continued)

LABEL	DESCRIPTION
IP Subnet Mask	This is the IP subnet mask of your Switch in dotted decimal notation for example 255.255.255.0.
Lease Time	This displays the length of time in seconds that this interface can use the current dynamic IP address from the DHCP server.
Renew Time	This displays the length of time from the lease start that the Switch will request to renew its current dynamic IP address from the DHCP server.
Rebind Time	This displays the length of time from the lease start that the Switch will request to get any dynamic IP address from the DHCP server.
Lease Time Start	This displays the date and time that the current dynamic IP address assignment from the DHCP server began. You should configure date and time in **Basic > General Setup**.
Lease Time End	This displays the date and time that the current dynamic IP address assignment from the DHCP server will end. You should configure date and time in **Basic > General Setup**.
Default Gateway	This displays the IP address of the default gateway assigned by the DHCP server. 0.0.0.0 means no gateway is assigned.
DNS Server	This displays the IP address of the primary and secondary DNS servers assigned by the DHCP server. 0.0.0.0 means no DNS server is assigned.

8.6.3 IP Configuration

Use this screen to configure IP-related settings.

8.6.3.1 IP Interfaces

The Switch needs an IP address for it to be managed over the network. The factory default IP address is 192.168.1.1. The subnet mask specifies the network number portion of an IP address. The factory default subnet mask is 255.255.255.0.

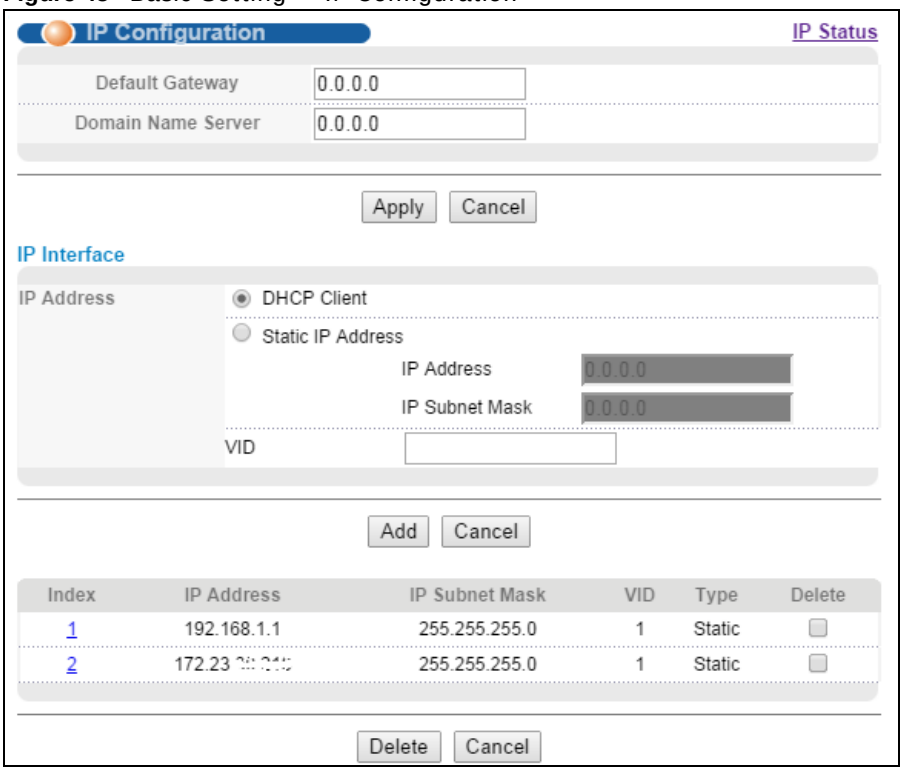
On the Switch, an IP address is not bound to any physical ports. Since each IP address on the Switch must be in a separate subnet, the configured IP address is also known as IP interface (or routing domain). In addition, this allows routing between subnets based on the IP address without additional routers.

You can configure multiple routing domains on the same VLAN as long as the IP address ranges for the domains do not overlap. To change the IP address of the Switch in a routing domain, simply add a new routing domain entry with a different IP address in the same subnet.

You can configure up to 32 IP domains which are used to access and manage the Switch from the ports belonging to the pre-defined VLAN(s).

Click **IP Setup > IP Configuration** to display the next screen.

Figure 45 Basic Setting > IP Configuration



The following table describes the labels in this screen.

Table 16 Basic Setting > IP Configuration

LABEL	DESCRIPTION
Default Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation.
Domain Name Server	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. Enter a domain name server IP address in order to be able to use a domain name instead of an IP address.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields.
IP Interface Use these fields to create or edit IP routing domains on the Switch. Each is the IP address of the Switch in an IP routing domain.	
DHCP Client	Select this option if you have a DHCP server that can assign the Switch an IP address, subnet mask, a default gateway IP address and a domain name server IP address automatically.
Static IP Address	Select this option if you don't have a DHCP server or if you wish to assign static IP address information to the Switch. You need to fill in the following fields when you select this option.
IP Address	Enter the IP address of your Switch in dotted decimal notation for example 192.168.1.1.
IP Subnet Mask	Enter the IP subnet mask of your Switch in dotted decimal notation for example 255.255.255.0.
VID	Enter the VLAN identification number to which an IP routing domain belongs.

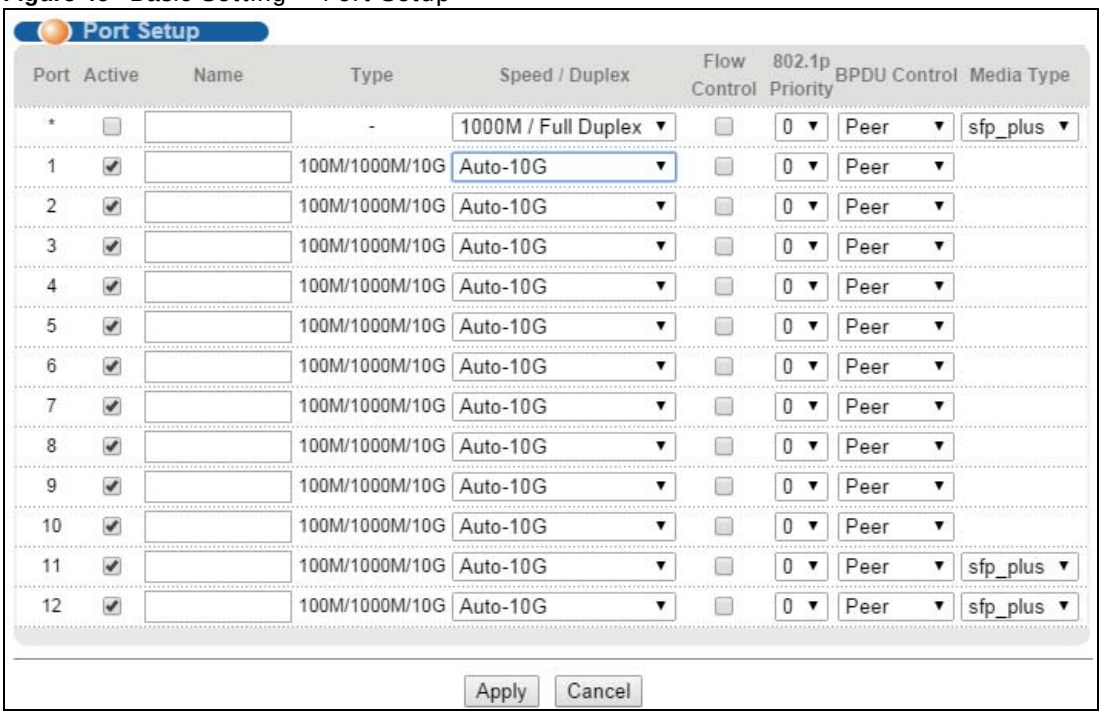
Table 16 Basic Setting > IP Configuration (continued)

LABEL	DESCRIPTION
Add	Click **Add** to insert the entry to the summary table below and save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to your previous configuration.
Summary Table	
Index	This field displays the index number of the rule. Click an index number to edit the rule.
IP Address	This field displays the IP address.
IP Subnet Mask	This field displays the subnet mask.
VID	This field displays the ID number of the VLAN group.
Type	This field displays whether this IP interface has a static or DHCP-assigned IP address.
Delete	Select the entries you want to remove.
Delete	Click **Delete** to remove the selected entry from the summary table. Note: Deleting all IP subnets locks you out of the Switch.
Cancel	Click **Cancel** to clear the selected check boxes in the **Delete** column.

8.7 Port Setup

Use this screen to configure Switch port settings. Click **Basic Setting** > **Port Setup** in the navigation panel to display the configuration screen.

Figure 46 Basic Setting > Port Setup



The following table describes the labels in this screen.

Table 17 Basic Setting > Port Setup

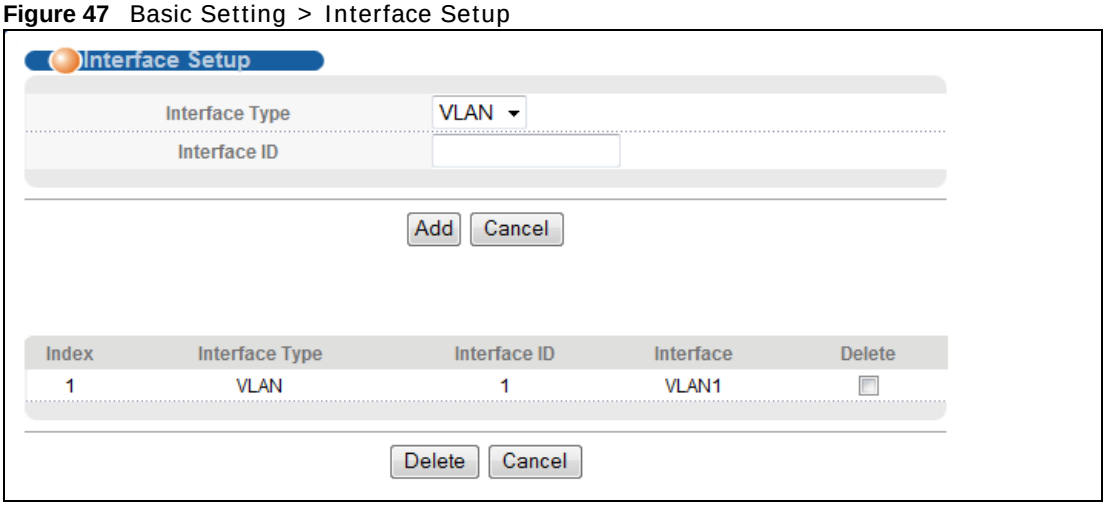
LABEL	DESCRIPTION
Port	This is the port index number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to enable a port. The factory default for all ports is enabled. A port must be enabled for data transmission to occur.
Name	Enter a descriptive name that identifies this port. You can enter up to 64 alpha-numerical characters. Note: Due to space limitation, the port name may be truncated in some web configurator screens.
Type	This field displays the capacity that the port can support.
Speed/Duplex	Select the speed and the duplex mode of the Ethernet connection on this port. Choices are **100M/Full Duplex** , **1000M/Full Duplex, 10G/Full Duplex, Auto-1000M / Full-Duplex, Auto-10G / Full Duplex**. **Auto-1000M / Full-Duplex** supports Ethernet and fiber connections at 100Mbps or 1000Mbps (1Gbps) full-duplex mode. **Auto-10G / Full-Duplex** supports Ethernet connections at 100Mbps, 1000Mbps or 10Gbps full-duplex mode and 10Gbps (only) for fiber connections. Selecting **Auto-1000M or Auto-10G** (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed that both ends support. When auto-negotiation is turned on, a port on the Switch negotiates with the peer automatically to determine the connection speed . If the peer port does not support auto-negotiation or turns off this feature, the Switch determines the connection speed by detecting the signal on the cablee. When the Switch's auto-negotiation is turned off, a port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect.
Flow Control	A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses. **Flow Control** is used to regulate transmission of signals to match the bandwidth of the receiving port. The Switch uses IEEE802.3x flow control in full duplex mode and backpressure flow control in half duplex mode. IEEE802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill. Back Pressure flow control is typically used to send a "collision" signal to the sending port (mimicking a state of packet collision) causing the sending port to temporarily stop sending signals and resend later. Select **Flow Control** to enable it.
802.1p Priority	This priority value is added to incoming frames without a (802.1p) priority queue tag. See **Priority Queue Assignment** in Table 12 on page 63 for more information.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

8.8 Interface Setup

An IPv6 address is configured on a per-interface basis. The interface can support virtual interface (for example, a VLAN). The Switch supports the VLAN interface type for IPv6 at the time of writing.

Use this screen to set IPv6 interfaces on which you can configure an IPv6 address to access and manage the Switch. Click **Basic Setting > Interface Setup** in the navigation panel to display the configuration screen.

Figure 47 Basic Setting > Interface Setup



The following table describes the labels in this screen.

Table 18 Basic Setting > Interface Setup

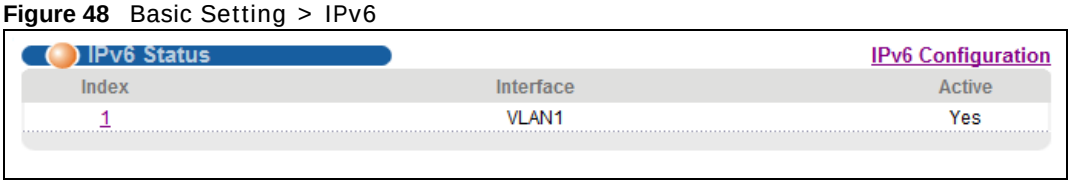
LABEL	DESCRIPTION
Interface Type	Select the type of IPv6 interface for which you want to configure. The Switch supports the VLAN interface type for IPv6 at the time of writing.
Interface ID	Specify a unique identification number (from 1 to 4094) for the interface. To have IPv6 function properly, you should configure a static VLAN with the same ID number in the **Advanced Application > VLAN** screens.
Add	Click this to create a new entry. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to your previous configuration.
Index	This field displays the index number of an entry.
Interface Type	This field displays the type of interface.
Interface ID	This field displays the identification number of the interface.
Interface	This field displays the interface's descriptive name which is generated automatically by the Switch. The name is from a combination of the interface type and ID number.
Delete	Check the rules that you want to remove in the delete column, then click the **Delete** button.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

8.9 IPv6

Use this screen to view the IPv6 interface status and configure Switch's management IPv6 addresses.

Click **Basic Setting** > **IPv6** in the navigation panel to display the IPv6 status screen as shown next.

Figure 48 Basic Setting > IPv6



The following table describes the labels in this screen.

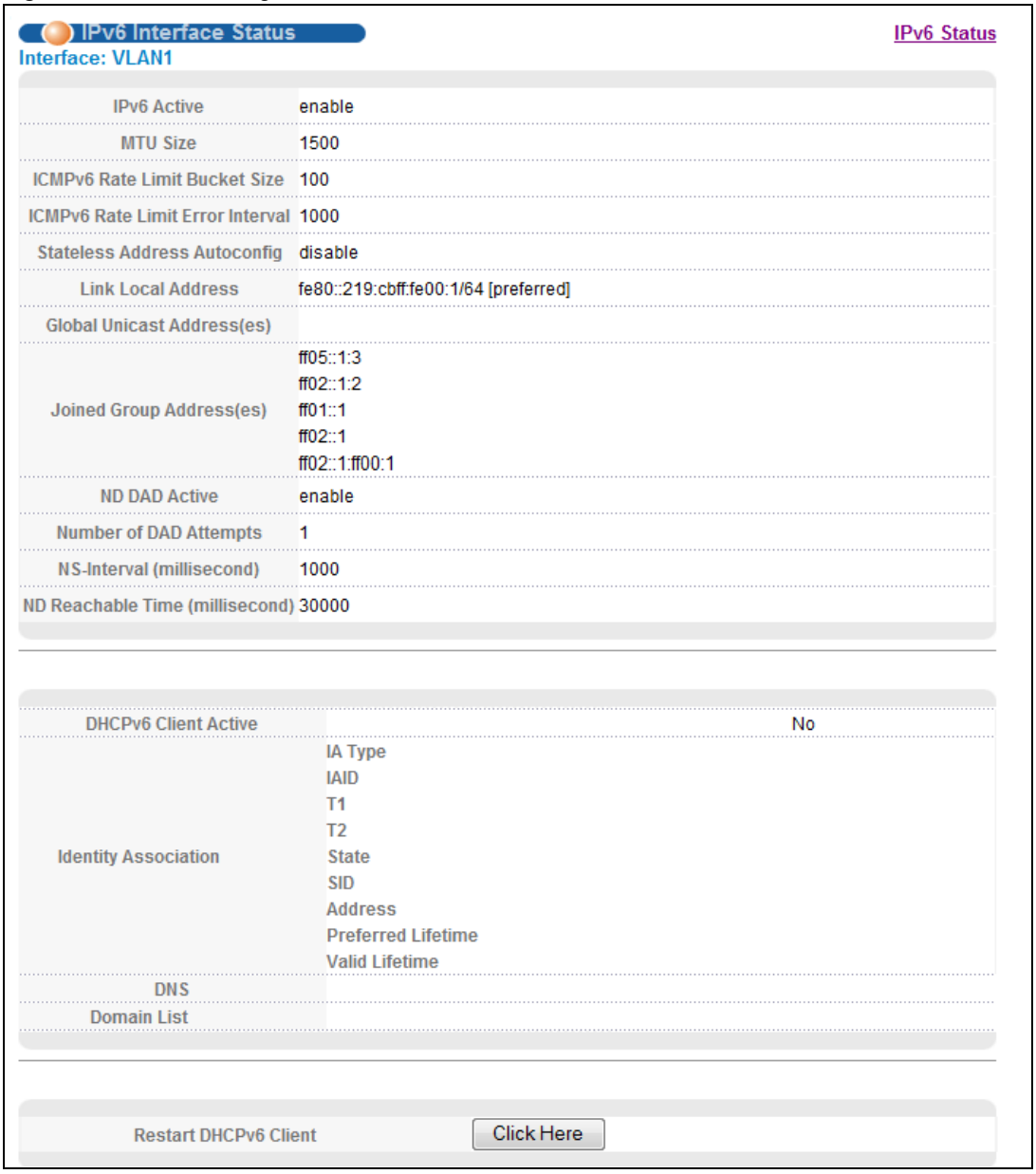
Table 19 Basic Setting > IPv6

LABEL	DESCRIPTION
Index	This field displays the index number of an IPv6 interface. Click on an index number to view more interface details.
Interface	This is the name of the IPv6 interface you created.
Active	This field displays whether the IPv6 interface is activated or not.

8.9.1 IPv6 Interface Status

Use this screen to view a specific IPv6 interface status and detailed information. Click an interface index number in the **Basic Setting** > **IPv6** screen. The following screen opens.

Figure 49 Basic Setting > IPv6 > IPv6 Interface Status



The following table describes the labels in this screen.

Table 20 Basic Setting > IPv6 > IPv6 Interface Status

LABEL	DESCRIPTION
IPv6 Active	This field displays whether the IPv6 interface is activated or not.
MTU Size	This field displays the Maximum Transmission Unit (MTU) size for IPv6 packets on this interface.
ICMPv6 Rate Limit Bucket Size	This field displays the maximum number of ICMPv6 error messages which are allowed to transmit in a given time interval. If the bucket is full, subsequent error messages are suppressed.
ICMPv6 Rate Limit Error Interval	This field displays the time period (in milliseconds) during which ICMPv6 error messages of up to the bucket size can be transmitted. 0 means no limit.

Table 20 Basic Setting > IPv6 > IPv6 Interface Status (continued)

LABEL	DESCRIPTION
Stateless Address Autoconfig	This field displays whether the Switch's interface can automatically generate a link-local address via stateless autoconfiguration.
Link Local Address	This field displays the Switch's link-local IP address and prefix generated by the interface. It also shows whether the IP address is preferred, which means it is a valid address and can be used as a sender or receiver address.
Global Unicast Address(es)	This field displays the Switch's global unicast address to identify this interface.
Joined Group Address(es)	This field displays the IPv6 multicast addresses of groups the Switch's interface joins.
ND DAD Active	This field displays whether Neighbor Discovery (ND) Duplicate Address Detection (DAD) is enabled on the interface.
Number of DAD Attempts	This field displays the number of consecutive neighbor solicitations the Switch sends for this interface.
NS-Interval (millisecond)	This field displays the time interval (in milliseconds) at which neighbor solicitations are re-sent for this interface.
ND Reachable Time (millisecond)	This field displays how long (in milliseconds) a neighbor is considered reachable for this interface.
DHCPv6 Client Active	This field displays whether the Switch acts as a DHCPv6 client to get an IPv6 address from a DHCPv6 server.
Identity Association	An Identity Association (IA) is a collection of addresses assigned to a DHCP client, through which the server and client can manage a set of related IP addresses. Each IA must be associated with exactly one interface.
IA Type	The IA type is the type of address in the IA. Each IA holds one type of address. **IA_NA** means an identity association for non-temporary addresses and **IA_TA** is an identity association for temporary addresses.
IAID	Each IA consists of a unique IAID and associated IP information.
T1	This field displays the DHCPv6 T1 timer. After T1, the Switch sends the DHCPv6 server a Renew message. An IA_NA option contains the T1 and T2 fields, but an IA_TA option does not. The DHCPv6 server uses T1 and T2 to control the time at which the client contacts with the server to extend the lifetimes on any addresses in the IA_NA before the lifetimes expire.
T2	This field displays the DHCPv6 T2 timer. If the time T2 is reached and the server does not respond, the Switch sends a Rebind message to any available server.
State	This field displays the state of the TA. It shows **Active** when the Switch obtains addresses from a DHCpv6 server and the TA is created. **Renew** when the TA's address lifetime expires and the Switch sends out a Renew message. **Rebind** when the Switch doesn't receive a response from the original DHCPv6 server and sends out a Rebind message to another DHCPv6 server.
SID	This field displays the DHCPv6 server's unique ID.
Address	This field displays the Switch's global address which is assigned by the DHCPv6 server.
Preferred Lifetime	This field displays how long (in seconds) that the global address remains preferred.
Valid Lifetime	This field displays how long (in seconds) that the global address is valid.
DNS	This field displays the DNS server address assigned by the DHCPv6 server.

Table 20 Basic Setting > IPv6 > IPv6 Interface Status (continued)

LABEL	DESCRIPTION
Domain List	This field displays the address record when the Switch queries the DNS server to resolve domain names.
Restart DHCPv6 Client	Click **Click Here** to send a new DHCP request to the DHCPv6 server and update the IPv6 address and DNS information for this interface.

8.9.2 IPv6 Configuration

Use this screen to configure IPv6 settings on the Switch. Click the **IPv6 Configuration** link in the **Basic Setting** > **IPv6** screen. The following screen opens.

Figure 50 Basic Setting > IPv6 > IPv6 Configuration

The following table describes the labels in this screen.

Table 21 Basic Setting > IPv6 > IPv6 Configuration

LABEL	DESCRIPTION
IPv6 Global Setup	Click the link to go to a screen where you can configure the global IPv6 settings on the Switch.
IPv6 Interface Setup	Click the link to go to a screen where you can enable an IPv6 interface on the Switch.
IPv6 Addressing	
IPv6 Link-Local Address Setup	Click the link to go to a screen where you can configure the IPv6 link-local address for an interface.
IPv6 Global Address Setup	Click the link to go to a screen where you can configure the IPv6 global address for an interface.
IPv6 Neighbor Discovery	
IPv6 Neighbor Discovery Setup	Click the link to go to a screen where you can configure the IPv6 neighbor discovery settings.

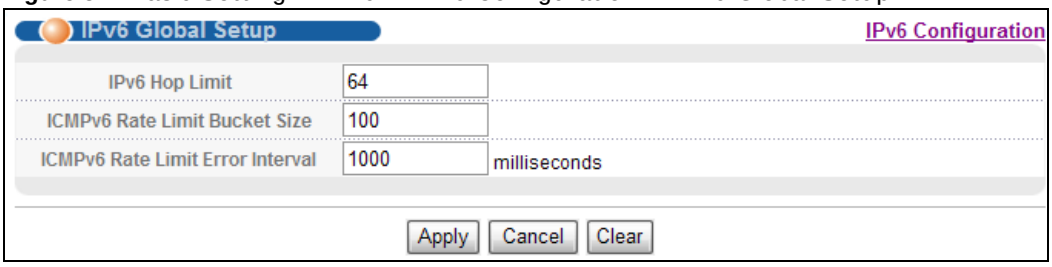
Table 21 Basic Setting > IPv6 > IPv6 Configuration (continued)

LABEL	DESCRIPTION
IPv6 Router Discovery Setup	Click the link to go to a screen where you can configure the IPv6 router discovery settings.
IPv6 Prefix Setup	Click the link to go to a screen where you can configure the IPv6 prefixy settings.
IPv6 Neighbor Setup	Click the link to go to a screen where you can create a static IPv6 neighbor entry in the Switch's IPv6 neighbor table.
DHCPv6 Client Setup	Click the link to go to a screen where you can configure the Switch DHCP settings.

8.9.3 IPv6 Global Setup

Use this screen to configure the global IPv6 settings. Click the link next to **IPv6 Global Setup** in the **IPv6 Configuration** screen to display the screen as shown next.

Figure 51 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Global Setup



The following table describes the labels in this screen.

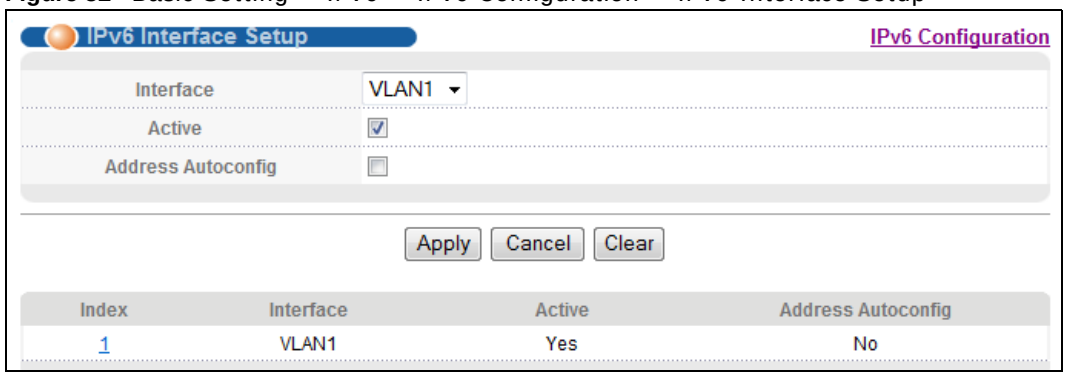
Table 22 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Global Setup

LABEL	DESCRIPTION
IPv6 Hop Limit	Specify the maximum number of hops (from 1 to 255) in router advertisements. This is the maximum number of hops on which an IPv6 packet is allowed to transmit before it is discarded by an IPv6 router, which is similar to the TTL field in IPv4.
ICMPv6 Rate Limit Bucket Size	Specify the maximum number of ICMPv6 error messages (from 1 to 200) which are allowed to transmit in a given time interval. If the bucket is full, subsequent error messages are suppressed.
ICMPv6 Rate Limit Error Interval	Specify the time period (from 0 to 2147483647 milliseconds) during which ICMPv6 error messages of up to the bucket size can be transmitted. 0 means no limit.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the nonvolatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to reset the fields to the factory defaults.

8.9.4 IPv6 Interface Setup

Use this screen to turn on or off an IPv6 interface and enable stateless autoconfiguration on it. Click the link next to **IPv6 Interface Setup** in the **IPv6 Configuration** screen to display the screen as shown next.

Figure 52 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Interface Setup



The following table describes the labels in this screen.

Table 23 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Interface Setup

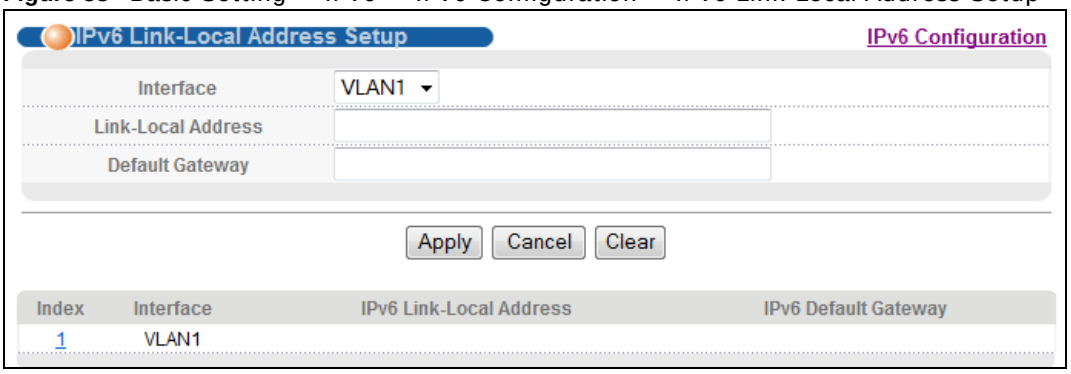
LABEL	DESCRIPTION
Interface	Select the IPv6 interface you want to configure.
Active	Select this option to enable the interface.
Address Autoconfig	Select this option to allow the interface to automatically generate a link-local address via stateless autoconfiguration.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the nonvolatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to reset the fields to the factory defaults.
Index	This is the interface index number. Click on an index number to change the settings.
Interface	This is the name of the IPv6 interface you created.
Active	This field displays whether the IPv6 interface is activated or not.
Address Autoconfig	This field displays whether stateless autoconfiguration is enabled on the interface.

8.9.5 IPv6 Link-Local Address Setup

A link-local address uniquely identifies a device on the local network (the LAN). It is similar to a "private IP address" in IPv4. You can have the same link-local address on multiple interfaces on a device. A link-local unicast address has a predefined prefix of fe80::/10.

Use this screen to configure the interface's link-local address and default gateway. Click the link next to **IPv6 Link-Local Address Setup** in the **IPv6 Configuration** screen to display the screen as shown next.

Figure 53 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Link-Local Address Setup



The following table describes the labels in this screen.

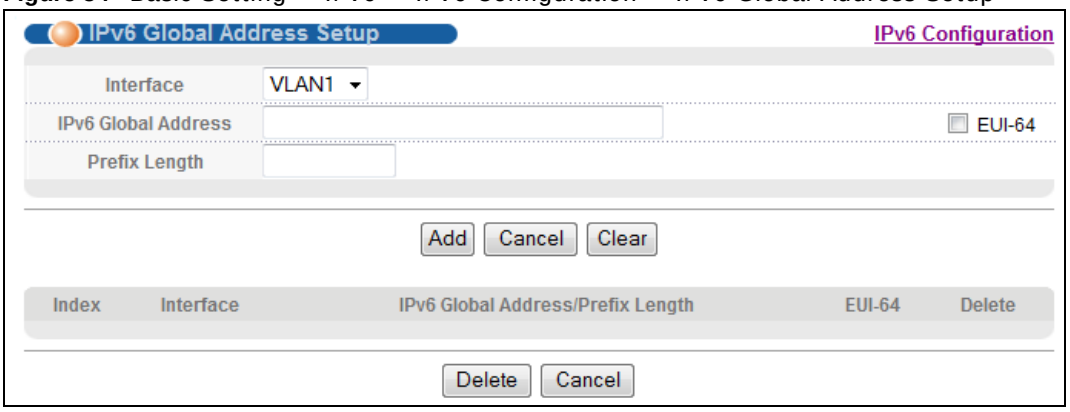
Table 24 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Link-Local Address Setup

LABEL	DESCRIPTION
Interface	Select the IPv6 interface you want to configure.
Link-Local Address	Manually configure a static IPv6 link-local address for the interface.
Default Gateway	Set the default gateway IPv6 address for the interface. When an interface cannot find a routing information for a frame's destination, it forwards the packet to the default gateway.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the nonvolatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to reset the fields to the factory defaults.
Index	This is the interface index number. Click on an index number to change the settings.
Interface	This is the name of the IPv6 interface you created.
IPv6 Link-Local Address	This is the static IPv6 link-local address for the interface.
IPv6 Default Gateway	This is the default gateway IPv6 address for the interface.

8.9.6 IPv6 Global Address Setup

Use this screen to configure the interface's IPv6 global address. Click the link next to **IPv6 Global Address Setup** in the **IPv6 Configuration** screen to display the screen as shown next.

Figure 54 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Global Address Setup



The following table describes the labels in this screen.

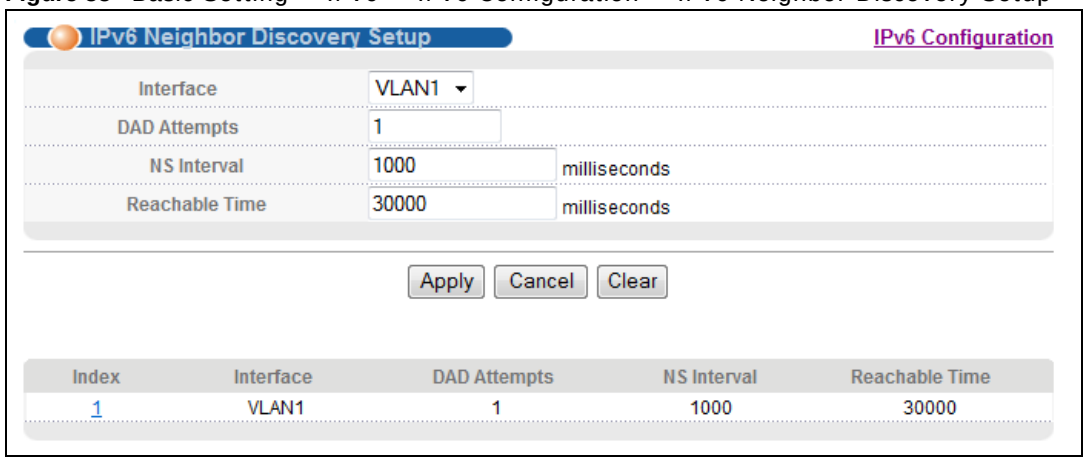
Table 25 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Global Address Setup

LABEL	DESCRIPTION
Interface	Select the IPv6 interface you want to configure.
IPv6 Global Address	Manually configure a static IPv6 global address for the interface.
Prefix Length	Specify an IPv6 prefix length that specifies how many most significant bits (start from the left) in the address compose the network address.
EUI-64	Select this option to have the interface ID be generated automatically using the EUI-64 format.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the nonvolatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to reset the fields to the factory defaults.
Index	This is the interface index number. Click on an index number to change the settings.
Interface	This is the name of the IPv6 interface you created.
IPv6 Global Address/Prefix Length	This field displays the IPv6 global address and prefix length for the interface.
EUI-64	This shows whether the interface ID of the global address is generated using the EUI-64 format.
Delete	Check the entry(ies) that you want to remove in the **Delete** column and then click **Delete** to remove the selected entry(ies) from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

8.9.7 IPv6 Neighbor Discovery Setup

Use this screen to configure neighbor discovery settings for each interface. Click the link next to **IPv6 Neighbor Discovery Setup** in the **IPv6 Configuration** screen to display the screen as shown next.

Figure 55 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Neighbor Discovery Setup



The following table describes the labels in this screen.

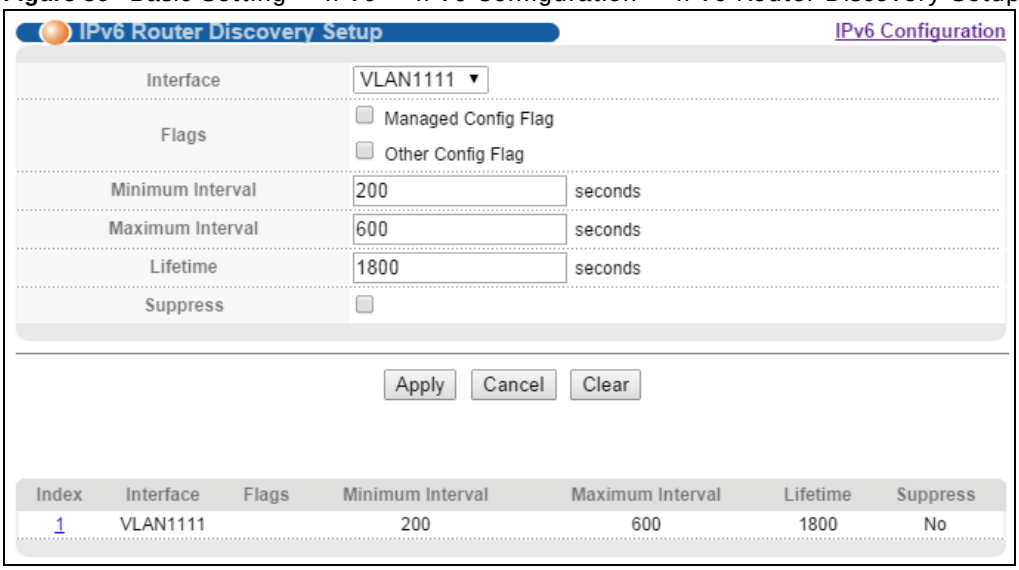
Table 26 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Neighbor Discovery Setup

LABEL	DESCRIPTION
Interface	Select the IPv6 interface you want to configure.
DAD Attempts	The Switch uses Duplicate Address Detection (DAD) with neighbor solicitation and advertisement messages to check whether an IPv6 address is already in use before assigning it to an interface, such as the link-local address it creates through stateless address autoconfiguration. Specify the number of consecutive neighbor solicitations (from 0 to 600) the Switch sends for this interface. Enter 0 to turn off DAD.
NS Interval	Specify the time interval (from 1000 to 3600000 milliseconds) at which neighbor solicitations are re-sent for this interface.
Reachable Time	Specify how long (from 1000 to 3600000 milliseconds) a neighbor is considered reachable for this interface.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the nonvolatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to reset the fields to the factory defaults.
Index	This is the interface index number. Click on an index number to change the settings.
Interface	This is the name of the IPv6 interface you created.
DAD Attempts	This field displays the number of consecutive neighbor solicitations the Switch sends for this interface.
NS Interval	This field displays the time interval (in milliseconds) at which neighbor solicitations are re-sent for this interface.
Reachable Time	This field displays how long (in milliseconds) a neighbor is considered reachable for this interface.

8.9.8 IPv6 Router Discovery Setup

Use this screen to configure router discovery settings for each interface. Click the link next to **IPv6 Router Discovery Setup** in the **IPv6 Configuration** screen to display the screen as shown next.

Figure 56 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Router Discovery Setup



The following table describes the labels in this screen.

Table 27 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Router Discovery Setup

LABEL	DESCRIPTION
Interface	Select the IPv6 interface you want to configure.
Flags	Select the **Managed Config Flag** option to have the Switch set the "managed address configuration" flag (the M flag) to 1 in IPv6 router advertisements, which means IPv6 hosts use DHCPv6 to obtain IPv6 stateful addresses. Deselect the option to set the flag to 0 and the host will not use DHCPv6 to obtain IPv6 stateful addresses. Select the **Other Config Flag** option to have the Switch set the "Other stateful configuration" flag (the O flag) to 1 in IPv6 router advertisements, which means IPv6 hosts use DHCPv6 to obtain additional configuration settings, such as DNS information. Deselect the option to set the flag to 0 and the host will not use DHCPv6 to obtain additional configuration settings.
Minimum Interval	Specify the minimum time interval (from 3 to 1350 seconds) at which the Switch sends router advertisements for this interface. Note: The minimum time interval cannot be greater than three-quarters of the maximum time interval.
Maximum Interval	Specify the maximum time interval (from 4 to 1800 seconds) at which the Switch sends router advertisements for this interface.
Lifetime	Specify how long (from 0 to 9000 seconds) the router in router advertisements can be used as a default router for this interface.
Suppress	Select this option to set the Switch to not send router advertisements and responses to router solicitations on this interface.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the nonvolatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to reset the fields to the factory defaults.
Index	This is the interface index number. Click on an index number to change the settings.
Interface	This is the name of the IPv6 interface you created.

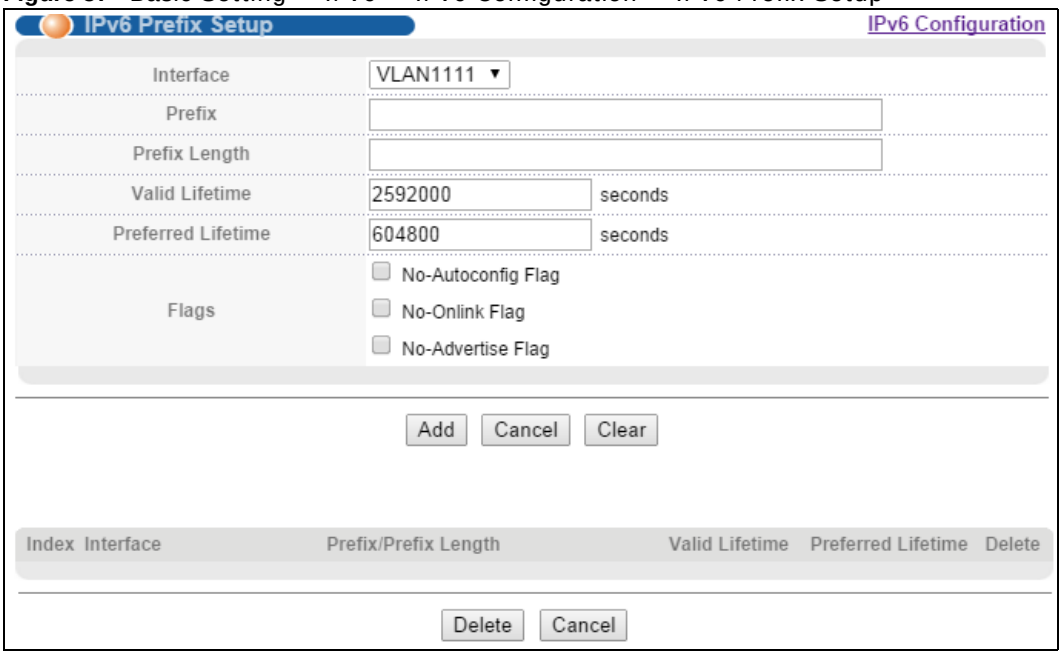
Table 27 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Router Discovery Setup (continued)

LABEL	DESCRIPTION
Flags	This field displays whether IPv6 hosts use DHCPv6 to obtain IPv6 stateful addresses (**M**) and/or additional configuration settings (**O**).
Minimum Interval	This field displays the minimum time interval at which the Switch sends router advertisements for this interface.
Maximum Interval	This field displays the maximum time interval at which the Switch sends router advertisements for this interface.
Lifetime	This field displays how long the router in router advertisements can be used as a default router for this interface.
Suppress	This field displays whether the Switch sends router advertisements and responses to router solicitations on this interface (**No**) or not (**Yes**).

8.9.9 IPv6 Prefix Setup

Use this screen to configure the Switch's IPv6 prefix list for each interface. Click the link next to **IPv6 Prefix Setup** in the **IPv6 Configuration** screen to display the screen as shown next.

Figure 57 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Prefix Setup



The following table describes the labels in this screen.

Table 28 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Prefix Setup

LABEL	DESCRIPTION
Interface	Select the IPv6 interface you want to configure.
Prefix	Set the IPv6 prefix that the Switch includes in router advertisements for this interface.
Prefix Length	Set the prefix length that the Switch includes in router advertisements for this interface.
Valid Lifetime	Specify how long (from 0 to 4294967295 seconds) the prefix is valid for on-link determination.

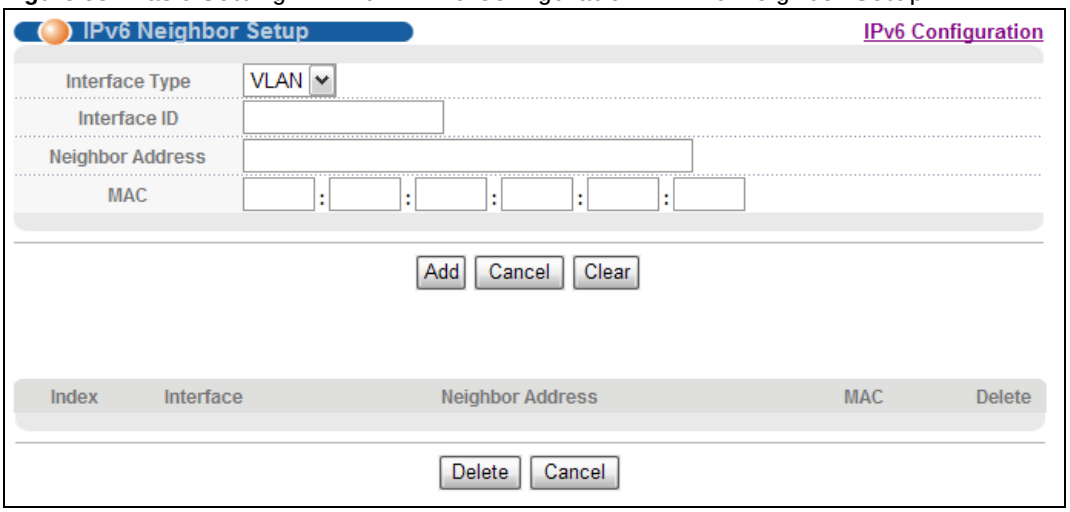
Table 28 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Prefix Setup (continued)

LABEL	DESCRIPTION
Preferred Lifetime	Specify how long (from 0 to 4294967295 seconds) that addresses generated from the prefix via stateless address autoconfiguration remain preferred. The preferred lifetime cannot exceed the valid lifetime.
Flags	Select **No-Autoconfig Flag** to not allow IPv6 hosts to use this prefix for stateless address autoconfiguration. Select **No-Onlink Flag** to not allow the specified prefix to be used for on-link determination. Select **No-Advertise Flag** to set the Switch to not include the specified IPv6 prefix, prefix length in router advertisements for this interface.
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the nonvolatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to reset the fields to the factory defaults.
Index	This is the interface index number. Click on an index number to change the settings.
Interface	This is the name of the IPv6 interface you created.
Prefix/Prefix Length	This field displays the IPv6 prefix and prefix length that the Switch includes in router advertisements for this interface.
Valid Lifetime	This field displays the IPv6 prefix valid lifetime.
Preferred Lifetime	This field displays the preferred lifetime of an IPv6 address generated from the prefix.
Delete	Check the entry(ies) that you want to remove in the **Delete** column and then click **Delete** to remove the selected entry(ies) from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

8.9.10 IPv6 Neighbor Setup

Use this screen to create a static IPv6 neighbor entry in the Switch's IPv6 neighbor table to store the neighbor information permanently. Click the link next to **IPv6 Neighbor Setup** in the **IPv6 Configuration** screen to display the screen as shown next.

Figure 58 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Neighbor Setup



The following table describes the labels in this screen.

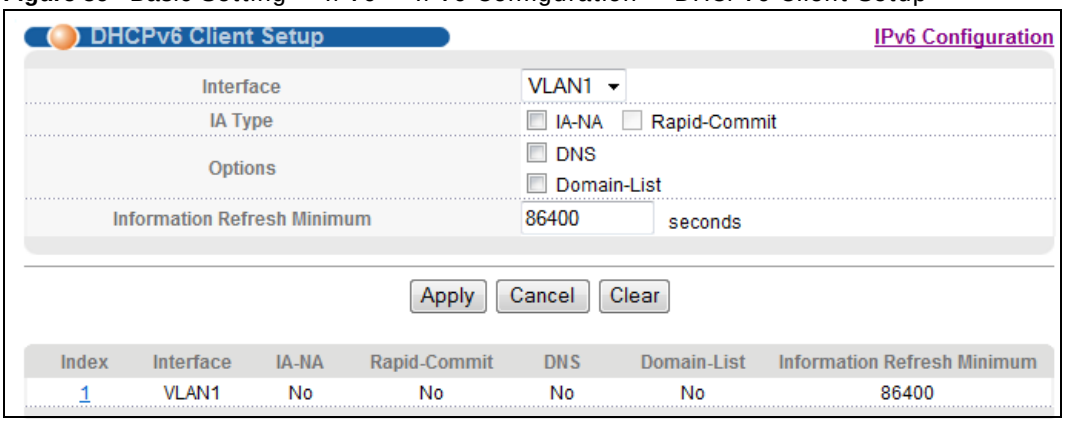
Table 29 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Neighbor Setup

LABEL	DESCRIPTION
Interface Type	Select the type of IPv6 interface for which you want to configure. The Switch supports the VLAN interface type for IPv6 at the time of writing.
Interface ID	Specify a unique identification number (from 1 to 4094) for the interface. A static IPv6 neighbor entry displays in the **Management > Neighbor Table** screen only when the interface ID is also created in the **Basic Setup > Interface Setup** screen. To have IPv6 function properly, you should configure a static VLAN with the same ID number in the **Advanced Application > VLAN** screens.
Neighbor Address	Specify the IPv6 address of the neighboring device which can be reached through the interface.
MAC	Specify the MAC address of the neighboring device which can be reached through the interface.
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the nonvolatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to reset the fields to the factory defaults.
Index	This is the interface index number. Click on an index number to change the settings.
Interface	This is the name of the IPv6 interface you created.
Neighbor Address	This field displays the IPv6 address of the neighboring device which can be reached through the interface
MAC	This field displays the MAC address of the neighboring device which can be reached through the interface.
Delete	Check the entry(ies) that you want to remove in the **Delete** column and then click **Delete** to remove the selected entry(ies) from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

8.9.11 DHCPv6 Client Setup

Use this screen to configure the Switch's DHCP settings when it is acting as a DHCPv6 client. Click the link next to **IPv6 Neighbor Setup** in the **IPv6 Configuration** screen to display the screen as shown next.

Figure 59 Basic Setting > IPv6 > IPv6 Configuration > DHCPv6 Client Setup



The following table describes the labels in this screen.

Table 30 Basic Setting > IPv6 > IPv6 Configuration > DHCPv6 Client Setup

LABEL	DESCRIPTION
Interface	Select the IPv6 interface you want to configure.
IA Type	Select **IA-NA** to set the Switch to get a non-temporary IP address from the DHCPv6 server for this interface. Optionally, you can also select **Rapid-Commit** to have the Switch send its DHCPv6 Solicit message with a Rapid Commit option to obtain information from the DHCPv6 server by a rapid two-message exchange. The Switch discards any Reply messages that do not include a Rapid Commit option. The DHCPv6 server should also support the Rapid Commit option to have it work well.
Options	Select **DNS** to have the Switch obtain DNS server IPv6 addresses and/or select **Domain-List** to have the Switch obtain a list of domain names from the DHCP server.
Information Refresh Minimum	Specify the time interval (from 600 to 4294967295 seconds) at which the Switch exchanges other configuration information with a DHCPv6 server again.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the nonvolatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to reset the fields to the factory defaults.
Index	This is the interface index number. Click on an index number to change the settings.
Interface	This is the name of the IPv6 interface you created.
IA-NA	This field displays whether the Switch obtains a non-temporary IP address from the DHCPv6 server.
Rapid-Commit	This field displays whether the Switch obtains information from the DHCPv6 server by a rapid two-message exchange.
DNS	This field displays whether the Switch obtains DNS server IPv6 addresses from the DHCPv6 server.
Domain-List	This field displays whether the Switch obtains a list of domain names from the DHCP server.
Information Refresh Minimum	This field displays the time interval (in seconds) at which the Switch exchanges other configuration information with a DHCPv6 server again.

9

VLAN

9.1 Overview

This chapter shows you how to configure 802.1Q tagged and port-based VLANs. The type of screen you see here depends on the **VLAN Type** you selected in the **Switch Setup** screen.

9.1.1 What You Can Do

- Use the **VLAN Status** screen (Section 9.2 on page 89) to view all VLAN groups.
- Use the **VLAN Detail** screen (Section 9.2.1 on page 90) to view detailed port settings and status of the VLAN group.
- Use the **Private VLAN Status** screen (Section 9.3 on page 91) to configure and view private VLANs for the Switch.
- Use the **VLAN Configuration** screen (Section 9.4 on page 92) to view VLAN screen options for the Switch.
- Use the **Static VLAN** screen (Section 9.5 on page 92) to configure and view 802.1Q VLAN parameters for the Switch.
- Use the **VLAN Port Setting** screen (Section 9.6 on page 94) to configure the static VLAN (IEEE 802.1Q) settings on a port.
- Use the **Subnet Based VLAN** screen (Section 9.7 on page 96) to set up VLANs that allow you to group traffic into logical VLANs based on the source IP subnet you specify.
- Use the **Protocol Based VLAN** screen (Section 9.8 on page 98) to set up VLANs that allow you to group traffic into logical VLANs based on the protocol you specify.
- Use the **Port-Based VLAN** screen (Section 9.9 on page 100) to set up VLANs where the packet forwarding decision is based on the destination MAC address and its associated port.
- Use the **Voice VLAN** screen (Section 9.9 on page 100) to set up VLANs that allow you to group voice traffic with defined priority and enable the switch port to carry the voice traffic separately from data traffic to ensure the sound quality does not deteriorate.
- Use **MAC-based VLAN** screen (Section 9.10 on page 102) to set up VLANs that allow you to group untagged packets into logical VLANs based on the source MAC address of the packet. This eliminates the need to reconfigure the switch when you change ports. The switch will forward the packets based on the source MAC address you setup previously.

9.1.2 What You Need to Know

Read this section to know more about VLAN and how to configure the screens.

IEEE 802.1Q Tagged VLANs

A tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges - they are not confined to the switch on which they were created. The

VLANs can be created statically by hand or dynamically through GVRP. The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. A tagged frame is four bytes longer than an untagged frame and contains two bytes of TPID (Tag Protocol Identifier, residing within the type/length field of the Ethernet frame) and two bytes of TCI (Tag Control Information, starts after the source address field of the Ethernet frame).

The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4,096 VLANs. Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

TPID	User Priority	CFI	VLAN ID
2 Bytes	3 Bits	1 Bit	12 bits

Forwarding Tagged and Untagged Frames

Each port on the Switch is capable of passing tagged or untagged frames. To forward a frame from an 802.1Q VLAN-aware switch to an 802.1Q VLAN-unaware switch, the Switch first decides where to forward the frame and then strips off the VLAN tag. To forward a frame from an 802.1Q VLAN-unaware switch to an 802.1Q VLAN-aware switch, the Switch first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port's default VID. The default PVID is VLAN 1 for all ports, but this can be changed.

A broadcast frame (or a multicast frame for a multicast group that is known by the system) is duplicated only on ports that are members of the VID (except the ingress port itself), thus confining the broadcast to a specific domain.

9.1.2.1 Automatic VLAN Registration

GARP and GVRP are the protocols used to automatically register VLAN membership across switches.

GARP

GARP (Generic Attribute Registration Protocol) allows network switches to register and de-register attribute values with other GARP participants within a bridged LAN. GARP is a protocol that provides a generic mechanism for protocols that serve a more specific application, for example, GVRP.

GARP Timers

Switches join VLANs by making a declaration. A declaration is made by issuing a Join message using GARP. Declarations are withdrawn by issuing a Leave message. A Leave All message terminates all registrations. GARP timers set declaration timeout values.

GVRP

GVRP (GARP VLAN Registration Protocol) is a registration protocol that defines a way for switches to register necessary VLAN members on ports across the network. Enable this function to permit VLAN groups beyond the local Switch.

Please refer to the following table for common IEEE 802.1Q VLAN terminology.

Table 31 IEEE 802.1Q VLAN Terminology

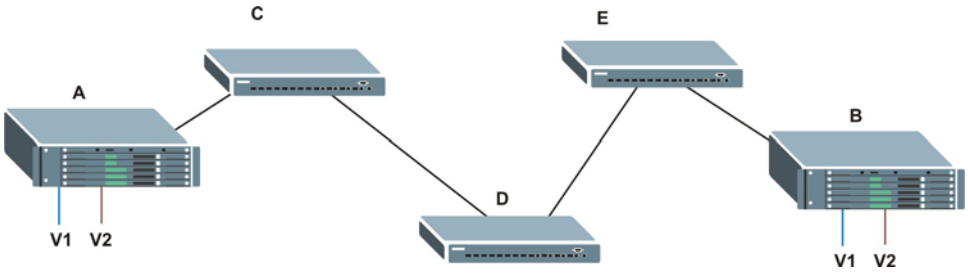
VLAN PARAMETER	TERM	DESCRIPTION
VLAN Type	Permanent VLAN	This is a static VLAN created manually.
	Dynamic VLAN	This is a VLAN configured by a GVRP registration/deregistration process.
VLAN Administrative Control	Registration Fixed	Fixed registration ports are permanent VLAN members.
	Registration Forbidden	Ports with registration forbidden are forbidden to join the specified VLAN.
	Normal Registration	Ports dynamically join a VLAN using GVRP.
VLAN Tag Control	Tagged	Ports belonging to the specified VLAN tag all outgoing frames transmitted.
	Untagged	Ports belonging to the specified VLAN don't tag all outgoing frames transmitted.
VLAN Port	Port VID	This is the VLAN ID assigned to untagged frames that this port received.
	Acceptable Frame Type	You may choose to accept both tagged and untagged incoming frames, just tagged incoming frames or just untagged incoming frames on a port.
	Ingress filtering	If set, the Switch discards incoming frames for VLANs that do not have this port as a member

9.1.2.2 Port VLAN Trunking

Enable **VLAN Trunking** on a port to allow frames belonging to unknown VLAN groups to pass through that port. This is useful if you want to set up VLAN groups on end devices without having to configure the same VLAN groups on intermediary devices.

Refer to the following figure. Suppose you want to create VLAN groups 1 and 2 (V1 and V2) on devices A and B. Without **VLAN Trunking**, you must configure VLAN groups 1 and 2 on all intermediary switches C, D and E; otherwise they will drop frames with unknown VLAN group tags. However, with **VLAN Trunking** enabled on a port(s) in each intermediary switch you only need to create VLAN groups in the end devices (A and B). C, D and E automatically allow frames with VLAN group tags 1 and 2 (VLAN groups that are unknown to those switches) to pass through their VLAN trunking port(s).

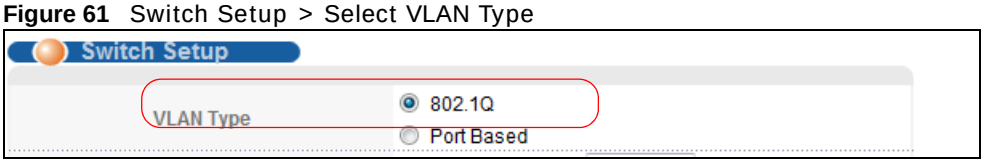
Figure 60 Port VLAN Trunking



9.1.2.3 Select the VLAN Type

Select a VLAN type in the **Basic Setting** > **Switch Setup** screen.

Figure 61 Switch Setup > Select VLAN Type



Static VLAN

Use a static VLAN to decide whether an incoming frame on a port should be

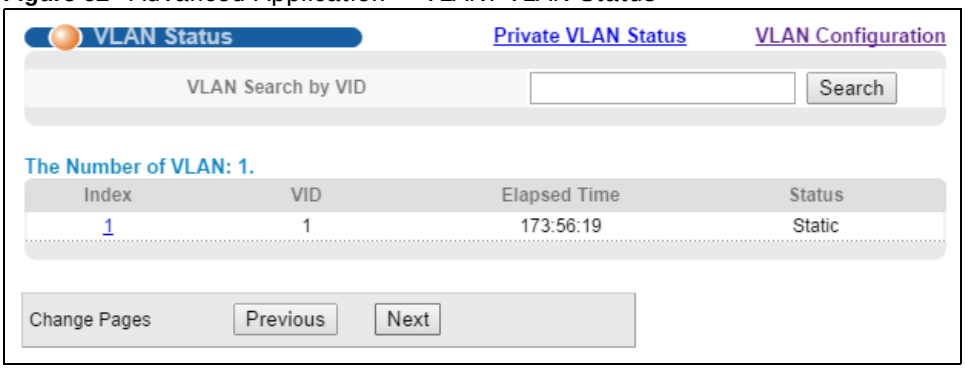
- sent to a VLAN group as normal depending on its VLAN tag.
- sent to a group whether it has a VLAN tag or not.
- blocked from a VLAN group regardless of its VLAN tag.

You can also tag all outgoing frames (that were previously untagged) from a port with the specified VID.

9.2 VLAN Status

Click **Advanced Application** > **VLAN** from the navigation panel to display the **VLAN Status** screen as shown next.

Figure 62 Advanced Application > VLAN: VLAN Status



The following table describes the labels in this screen.

Table 32 Advanced Application > VLAN: VLAN Status

LABEL	DESCRIPTION
VLAN Search by VID	Enter an existing VLAN ID number(s) (separated by a comma) and click **Search** to display only the specified VLAN(s) in the list below. Leave this field blank and click **Search** to display all VLANs configured on the Switch.
The Number of VLAN	This is the number of VLANs configured on the Switch.

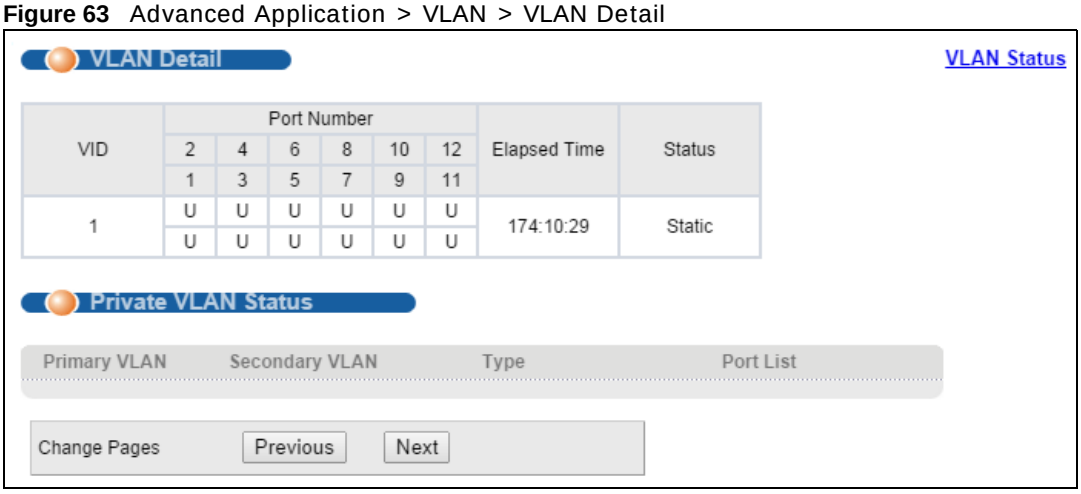
Table 32 Advanced Application > VLAN: VLAN Status (continued)

LABEL	DESCRIPTION
The Number of Search Results	This is the number of VLANs that match the searching criteria and display in the list below. This field displays only when you use the **Search** button to look for certain VLANs.
Index	This is the VLAN index number. Click on an index number to view more VLAN details.
VID	This is the VLAN identification number that was configured in the **Static VLAN** screen.
Elapsed Time	This field shows how long it has been since a normal VLAN was registered or a static VLAN was set up.
Status	This field shows how this VLAN was added to the Switch. • **Dynamic** - using GVRP • **Static** - manually added as a normal VLAN • **Private** - manually added as a private VLAN (primary, isolated or community) • **Voice** - manually added as a Voice VLAN • **MVR** - added via Multicast VLAN Registration (MVR)
Change Pages	Click **Previous** or **Next** to show the previous/next screen if all status information cannot be seen in one screen.

9.2.1 VLAN Details

Use this screen to view detailed port settings and status of the VLAN group. Click on an index number in the **VLAN Status** screen to display VLAN details.

Figure 63 Advanced Application > VLAN > VLAN Detail



The following table describes the labels in this screen.

Table 33 Advanced Application > VLAN > VLAN Detail

LABEL	DESCRIPTION
VLAN Status	Click this to go to the **VLAN Status** screen.
VID	This is the VLAN identification number that was configured in the **Static VLAN** screen.
Port Number	This column displays the ports that are participating in a VLAN. A tagged port is marked as **T**, an untagged port is marked as **U** and ports not participating in a VLAN are marked as "**–**".
Elapsed Time	This field shows how long it has been since a normal VLAN was registered or a static VLAN was set up.

Table 33 Advanced Application > VLAN > VLAN Detail (continued)

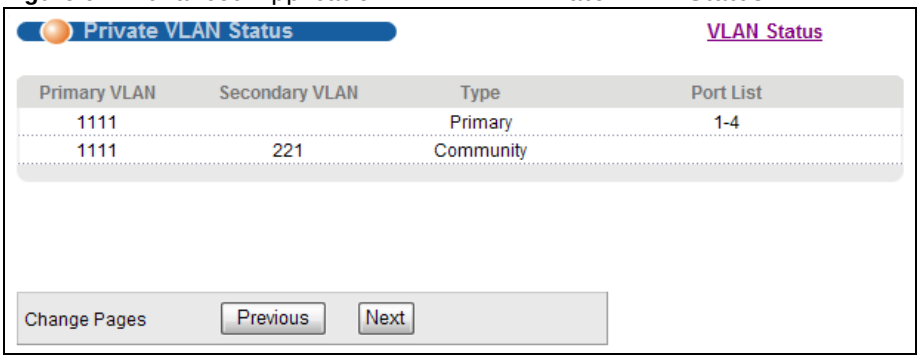
LABEL	DESCRIPTION
Status	This field shows how this VLAN was added to the Switch. • **Dynamic** - using GVRP • **Static** - manually added as a normal VLAN • **Private** - manually added as a private VLAN (primary, isolated or community) • **Voice** - manually added as a Voice VLAN • **MVR** - added via Multicast VLAN Registration (MVR)
Private VLAN Status	These fields show private VLAN information for the selected VLAN. See Section 9.3 on page 91 for related information on private VLANs.
Primary VLAN	This field shows the primary VLAN ID in the selected VLAN.
Secondary VLAN	This field shows the secondary VLAN ID in the selected VLAN.
Type	This field shows the type of private VLAN: **Primary**, **Community** or **Isolated**.
Port List	This shows the ports mapped to the private VLAN using the **Advanced Application > Private VLAN** or **Advanced Application > VLAN > Static VLAN** screen.
Change Pages	Click **Previous** or **Next** to show the previous/next screen if all status information cannot be seen in one screen.

9.3 Private VLAN Status

Use this screen to view all private VLANs created on the Switch. See also **Advanced Application > Private VLAN**.

Click **Private VLAN Status** in the **VLAN Status** screen to display the screen as shown next.

Figure 64 Advanced Application > VLAN > Private VLAN Status



The following table describes the labels in this screen.

Table 34 Advanced Application > VLAN > Private VLAN Status

LABEL	DESCRIPTION
Private VLAN Status	These fields show information for the all private VLANs. See also **Advanced Application > Private VLAN**.
Primary VLAN	This field shows the primary VLAN ID in a private VLAN.
Secondary VLAN	This field shows the secondary VLAN ID in a private VLAN.

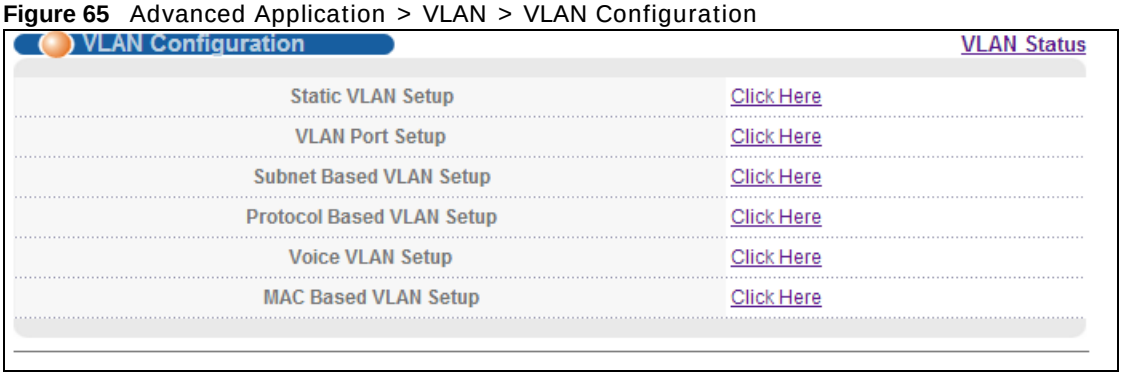
Table 34 Advanced Application > VLAN > Private VLAN Status (continued)

LABEL	DESCRIPTION
Type	This field shows the type of private VLAN: **Primary**, **Community** or **Isolated**.
Port List	This shows the ports mapped to the private VLAN using the **Advanced Application > Private VLAN** or **Advanced Application > VLAN > Static VLAN** screen.
Change Pages	Use the **Previous** and **Next** buttons to display different pages.

9.4 VLAN Configuration

Use this screen to view IEEE 802.1Q VLAN parameters for the Switch. Click **Advanced Application > VLAN > VLAN Configuration** to see the following screen.

Figure 65 Advanced Application > VLAN > VLAN Configuration



The following table describes the labels in the above screen.

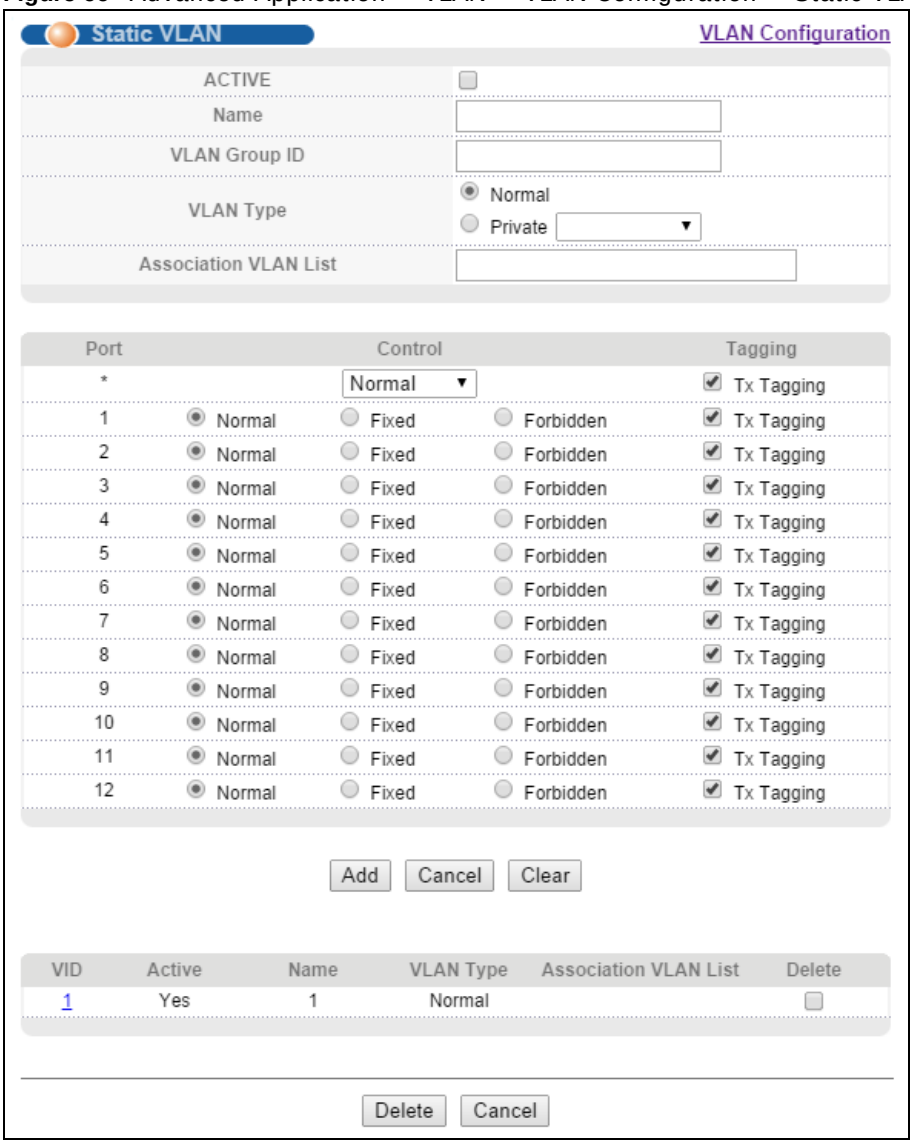
Table 35 Advanced Application > VLAN > VLAN Configuration

LABEL	DESCRIPTION
Static VLAN Setup	Click **Click Here** to configure the Static VLAN for the Switch.
VLAN Port Setup	Click **Click Here** to configure the VLAN Port for the Switch.
Subnet Based VLAN Setup	Click **Click Here** to configure the Subnet Based VLAN for the Switch.
Protocol Based VLAN Setup	Click **Click Here** to configure the Protocol Based VLAN for the Switch.
Voice VLAN Setup	Click **Click Here** to configure the Voice VLAN for the Switch.
MAC Based VLAN Setup	Click **Click Here** to configure the MAC Based VLAN for the Switch.

9.5 Configure a Static VLAN

Use this screen to configure a static VLAN for the Switch. Click **Static VLAN** in the **VLAN Status** screen to display the screen as shown next.

Figure 66 Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup



The following table describes the related labels in this screen.

Table 36 Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup

LABEL	DESCRIPTION
ACTIVE	Select this check box to activate the VLAN settings.
Name	Enter a descriptive name for the VLAN group for identification purposes. This name consists of up to 64 printable characters.
VLAN Group ID	Enter the VLAN ID for this static entry; the valid range is between 1 and 4094.
VLAN Type	Select **Normal** (static) or **Private**. For **Private** VLANs, select **Primary**, **Isolated** or **Community**.

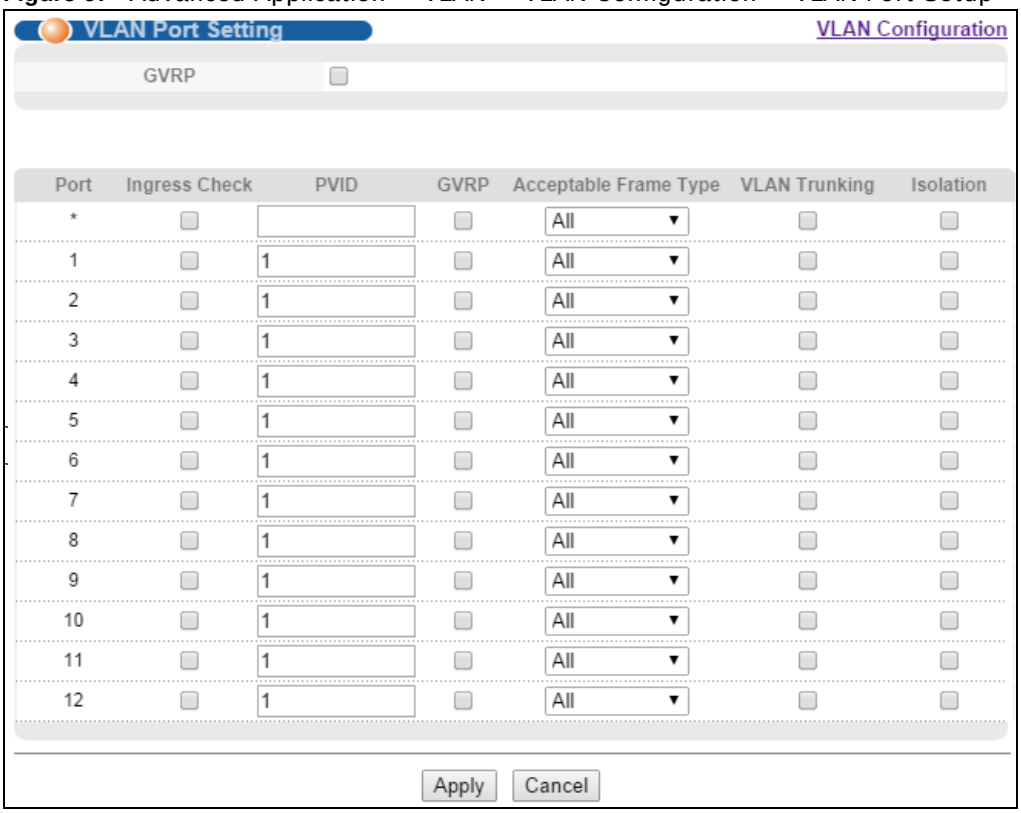
Table 36 Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup (continued)

LABEL	DESCRIPTION
Association VLAN List	**Primary** private VLANs can associate with several (secondary) **Community** private VLANs and up to one (secondary) **Isolated** private VLAN. You only configure **VLAN Association List** for **Primary** private VLANs. Use a dash to associate consecutive VLANs and a comma (no spaces) to associate non-consecutive VLANs. For example, 51-53 includes 51, 52 and 53, but 51,53 does not include 52. Secondary private VLANs can only be associated with one primary private VLAN.
Port	The port number identifies the port you are configuring.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Control	Select **Normal** for the port to dynamically join this VLAN group using GVRP. This is the default selection. Select **Fixed** for the port to be a permanent member of this VLAN group. Select **Forbidden** if you want to prohibit the port from joining this VLAN group.
Tagging	Select **TX Tagging** if you want the port to tag all outgoing frames transmitted with this VLAN Group ID.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to change the fields back to their last saved values.
Clear	Click **Clear** to start configuring the screen again.
VID	This field displays the ID number of the VLAN group. Click the number to edit the VLAN settings.
Active	This field indicates whether the VLAN settings are enabled (**Yes**) or disabled (**No**).
Name	This field displays the descriptive name for this VLAN group.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

9.6 Configure VLAN Port Settings

Use the VLAN Port Setting screen to configure the static VLAN (IEEE 802.1Q) settings on a port. Click the **VLAN Port Setup** link in the **VLAN Status** screen.

Figure 67 Advanced Application > VLAN > VLAN Configuration > VLAN Port Setup



The following table describes the labels in this screen.

Table 37 Advanced Application > VLAN > VLAN Configuration > VLAN Port Setup

LABEL	DESCRIPTION
GVRP	GVRP (GARP VLAN Registration Protocol) is a registration protocol that defines a way for switches to register necessary VLAN members on ports across the network. Select this check box to permit VLAN groups beyond the local Switch.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Ingress Check	If this check box is selected, the Switch discards incoming frames on a port for VLANs that do not include this port in its member set. Clear this check box to disable ingress filtering.
PVID	A PVID (Port VLAN ID) is a tag that adds to incoming untagged frames received on a port so that the frames are forwarded to the VLAN group that the tag defines. Enter a number between 1and 4094 as the port VLAN ID.
GVRP	Select this check box to allow GVRP on this port.

Table 37 Advanced Application > VLAN > VLAN Configuration > VLAN Port Setup

LABEL	DESCRIPTION
Acceptable Frame Type	Specify the type of frames allowed on a port. Choices are **All**, **Tag Only** and **Untag Only**. Select **All** from the drop-down list box to accept all untagged or tagged frames on this port. This is the default setting. Select **Tag Only** to accept only tagged frames on this port. All untagged frames will be dropped. Select **Untag Only** to accept only untagged frames on this port. All tagged frames will be dropped.
VLAN Trunking	Enable **VLAN Trunking** on ports connected to other switches or routers (but not ports directly connected to end users) to allow frames belonging to unknown VLAN groups to pass through the Switch.
Isolation	Select this to allows this port to communicate only with the CPU management port and the ports on which the isolation feature is not enabled.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

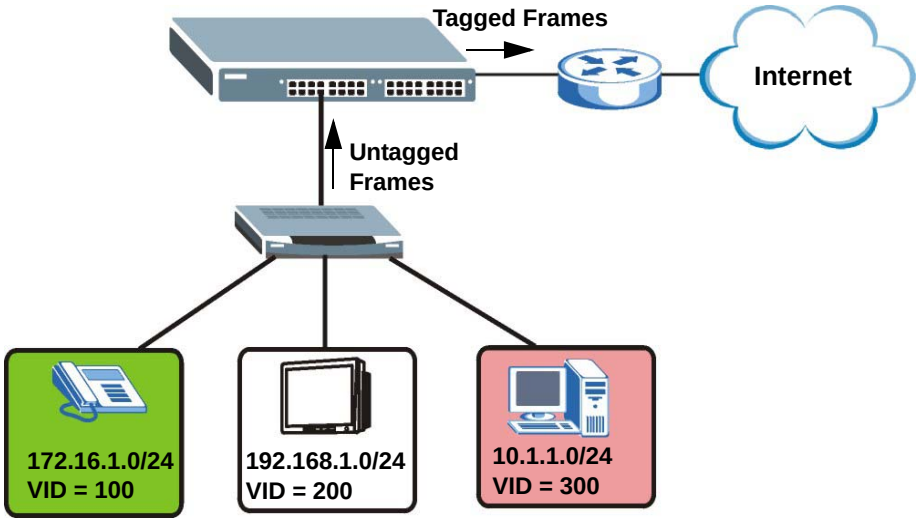
9.7 Subnet Based VLANs

Subnet based VLANs allow you to group traffic into logical VLANs based on the source IP subnet you specify. When a frame is received on a port, the Switch checks if a tag is added already and the IP subnet it came from. The untagged packets from the same IP subnet are then placed in the same subnet based VLAN. One advantage of using subnet based VLANs is that priority can be assigned to traffic from the same IP subnet.

For example, an ISP (Internet Services Provider) may divide different types of services it provides to customers into different IP subnets. Traffic for voice services is designated for IP subnet 172.16.1.0/24, video for 192.168.1.0/24 and data for 10.1.1.0/24. The Switch can then be configured to group incoming traffic based on the source IP subnet of incoming frames.

You configure a subnet based VLAN with priority 6 and VID of 100 for traffic received from IP subnet 172.16.1.0/24 (voice services). You also have a subnet based VLAN with priority 5 and VID of 200 for traffic received from IP subnet 192.168.1.0/24 (video services). Lastly, you configure VLAN with priority 3 and VID of 300 for traffic received from IP subnet 10.1.1.0/24 (data services). All untagged incoming frames will be classified based on their source IP subnet and prioritized accordingly. That is video services receive the highest priority and data the lowest.

Figure 68 Subnet Based VLAN Application Example

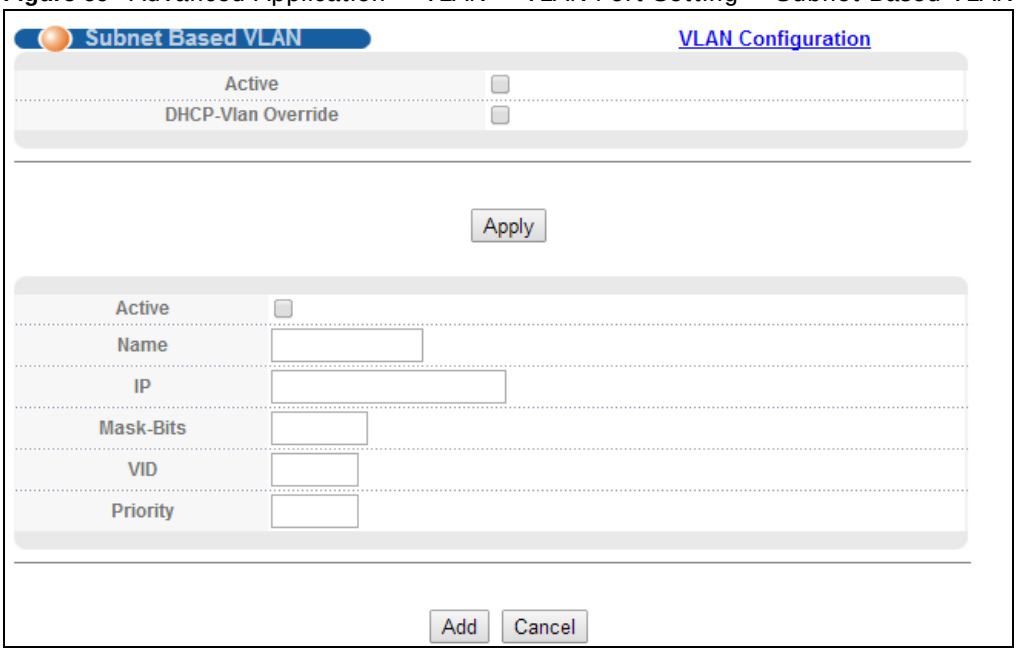


9.7.1 Configuring Subnet Based VLAN

Click **Subnet Based VLAN** in the **VLAN Port Setting** screen to display the configuration screen as shown.

Note: Subnet based VLAN applies to un-tagged packets and is applicable only when you use IEEE 802.1Q tagged VLAN.

Figure 69 Advanced Application > VLAN > VLAN Port Setting > Subnet Based VLAN



The following table describes the labels in this screen.

Table 38 Advanced Application > VLAN > VLAN Port Setting > Subnet Based VLAN Setup

LABEL	DESCRIPTION
Active	Check this box to activate this subnet based VLANs on the Switch.
DHCP-Vlan Override	When DHCP snooping is enabled DHCP clients can renew their IP address through the DHCP VLAN or via another DHCP server on the subnet based VLAN. Select this checkbox to force the DHCP clients in this IP subnet to obtain their IP addresses through the DHCP VLAN.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Active	Check this box to activate the IP subnet VLAN you are creating or editing.
Name	Enter up to 32 alpha numeric characters to identify this subnet based VLAN.
IP	Enter the IP address of the subnet for which you want to configure this subnet based VLAN.
Mask-Bits	Enter the bit number of the subnet mask. To find the bit number, convert the subnet mask to binary format and add all the 1's together. Take "255.255.255.0" for example. 255 converts to eight 1s in binary. There are three 255s, so add three eights together and you get the bit number (24).
VID	Enter the ID of a VLAN with which the untagged frames from the IP subnet specified in this subnet based VLAN are tagged. This must be an existing VLAN which you defined in the **Advanced Applications** > **VLAN** screens.
Priority	Select the priority level that the Switch assigns to frames belonging to this VLAN.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Index	This is the index number identifying this subnet based VLAN. Click on any of these numbers to edit an existing subnet based VLAN.
Active	This field shows whether the subnet based VLAN is active or not.
Name	This field shows the name the subnet based VLAN.
IP	This field shows the IP address of the subnet for this subnet based VLAN.
Mask-Bits	This field shows the subnet mask in bit number format for this subnet based VLAN.
VID	This field shows the VLAN ID of the frames which belong to this subnet based VLAN.
Priority	This field shows the priority which is assigned to frames belonging to this subnet based VLAN.
Delete	Click this to delete the subnet based VLANs which you marked for deletion.
Cancel	Click **Cancel** to begin configuring this screen afresh.

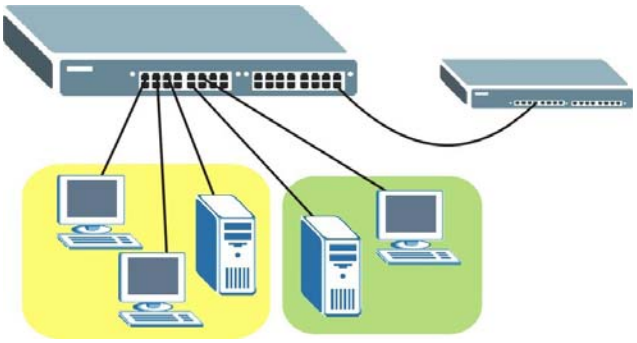
9.8 Protocol Based VLANs

Protocol based VLANs allow you to group traffic into logical VLANs based on the protocol you specify. When an upstream frame is received on a port (configured for a protocol based VLAN), the Switch checks if a tag is added already and its protocol. The untagged packets of the same protocol are then placed in the same protocol based VLAN. One advantage of using protocol based VLANs is that priority can be assigned to traffic of the same protocol.

Note: Protocol based VLAN applies to un-tagged packets and is applicable only when you use IEEE 802.1Q tagged VLAN.

For example, port 1, 2, 3 and 4 belong to static VLAN 100, and port 4, 5, 6, 7 belong to static VLAN 120. You configure a protocol based VLAN A with priority 3 for ARP traffic received on port 1, 2 and 3. You also have a protocol based VLAN B with priority 2 for Apple Talk traffic received on port 6 and 7. All upstream ARP traffic from port 1, 2 and 3 will be grouped together, and all upstream Apple Talk traffic from port 6 and 7 will be in another group and have higher priority than ARP traffic, when they go through the uplink port to a backbone switch C.

Figure 70 Protocol Based VLAN Application Example

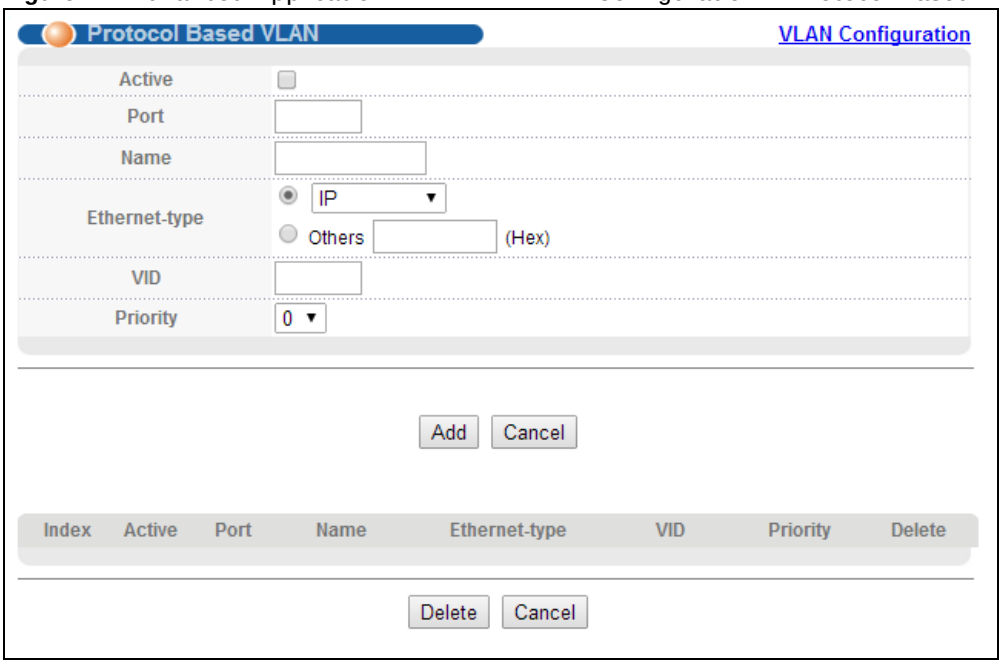


9.8.1 Configuring Protocol Based VLAN

Click **Protocol Based VLAN Setup** in the **VLAN Configuration** screen to display the configuration screen as shown.

Note: Protocol-based VLAN applies to un-tagged packets and is applicable only when you use IEEE 802.1Q tagged VLAN.

Figure 71 Advanced Application > VLAN > VLAN Configuration > Protocol Based VLAN Setup



The following table describes the labels in this screen.

Table 39 Advanced Application > VLAN > VLAN Configuration > Protocol Based VLAN Setup

LABEL	DESCRIPTION
Active	Check this box to activate this protocol based VLAN.
Port	Type a port to be included in this protocol based VLAN. This port must belong to a static VLAN in order to participate in a protocol based VLAN. See Chapter 9 on page 86 for more details on setting up VLANs.
Name	Enter up to 32 alpha numeric characters to identify this protocol based VLAN.
Ethernet-type	Use the drop down list box to select a predefined protocol to be included in this protocol based VLAN or select **Others** and type the protocol number in hexadecimal notation. For example the IP protocol in hexadecimal notation is 0800, and Novell IPX protocol is 8137. Note: Protocols in the hexadecimal number range of 0x0000 to 0x05ff are not allowed to be used for protocol based VLANs.
VID	Enter the ID of a VLAN to which the port belongs. This must be an existing VLAN which you defined in the **Advanced Applications** > **VLAN** screens.
Priority	Select the priority level that the Switch will assign to frames belonging to this VLAN.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Index	This is the index number identifying this protocol based VLAN. Click on any of these numbers to edit an existing protocol based VLAN.
Active	This field shows whether the protocol based VLAN is active or not.
Port	This field shows which port belongs to this protocol based VLAN.
Name	This field shows the name the protocol based VLAN.
Ethernet Type	This field shows which Ethernet protocol is part of this protocol based VLAN.
VID	This field shows the VLAN ID of the port.
Priority	This field shows the priority which is assigned to frames belonging to this protocol based VLAN.
Delete	Click this to delete the protocol based VLANs which you marked for deletion.
Cancel	Click **Cancel** to begin configuring this screen afresh.

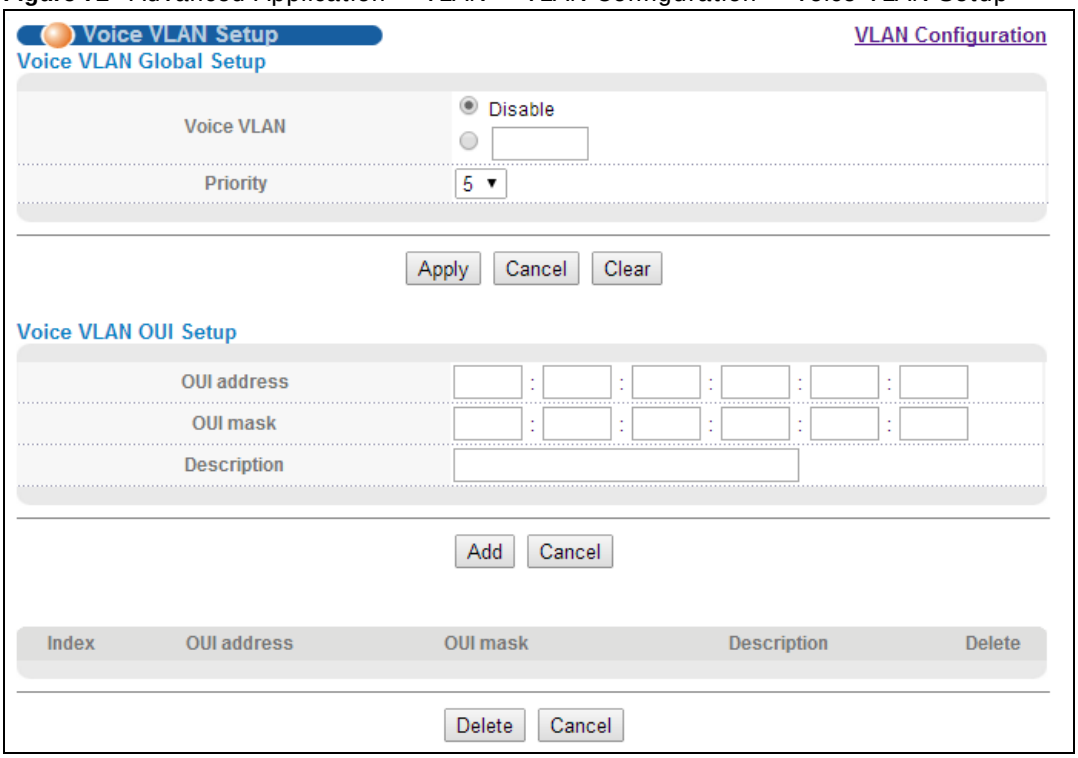
9.9 Voice VLAN

Voice VLAN ensures that the sound quality of an IP phone is preserved from deteriorating when the data traffic on the Switch ports is high. It groups the voice traffic with defined priority into an assigned VLAN which enables the separation of voice and data traffic coming onto the Switch port.

You can set priority level to the Voice VLAN and add MAC address of IP phones from specific manufacturers by using its ID from the Organizationally Unique Identifiers (OUI).

Click **Voice VLAN** in the **VLAN Configuration** screen to display the configuration screen as shown.

Figure 72 Advanced Application > VLAN > VLAN Configuration > Voice VLAN Setup



The following table describes the fields in the above screen.

Table 40 Advanced Application > VLAN > VLAN Configuration > Voice VLAN Setup

LABEL	DESCRIPTION
Voice VLAN Global Setup	
Voice VLAN	Click the Voice VLAN radio button if you want to enable the Voice VLAN feature. Type a VLAN ID number in the box next to the radio button that is associated with the Voice VLAN. Click **Disable** radio button if you do not want to enable the Voice VLAN feature.
Priority	Select the priority level of the Voice VLAN from 0 to 7. Default setting is 5.The higher the numeric value you assign, the higher the priority for this Voice VLAN.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to reset the fields to default settings.
Voice VLAN OUI Setup	
OUI address	Type the IP Phone manufacturer's OUI MAC address. The first three byes is the manufacturer identifier, the last three bytes is a unique station ID.
OUI mask	Type the IP Phone manufacturer's OUI mask address.
Description	Type an description up to 32 characters for the Voice VLAN device. For example: Siemens.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.

Table 40 Advanced Application > VLAN > VLAN Configuration > Voice VLAN Setup

LABEL	DESCRIPTION
Cancel	Click **Cancel** to begin configuring this screen afresh.
Index	This field displays the index number of the Voice VLAN.
OUI address	This field displays the OUI address of the Voice VLAN.
OUI mask	This field displays the OUI mask address of the Voice VLAN.
Description	This field displays the description of the Voice VLAN with OUI address.
Delete	Click the **Delete** check box to select Voice VLAN OUI entry you wish to remove.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

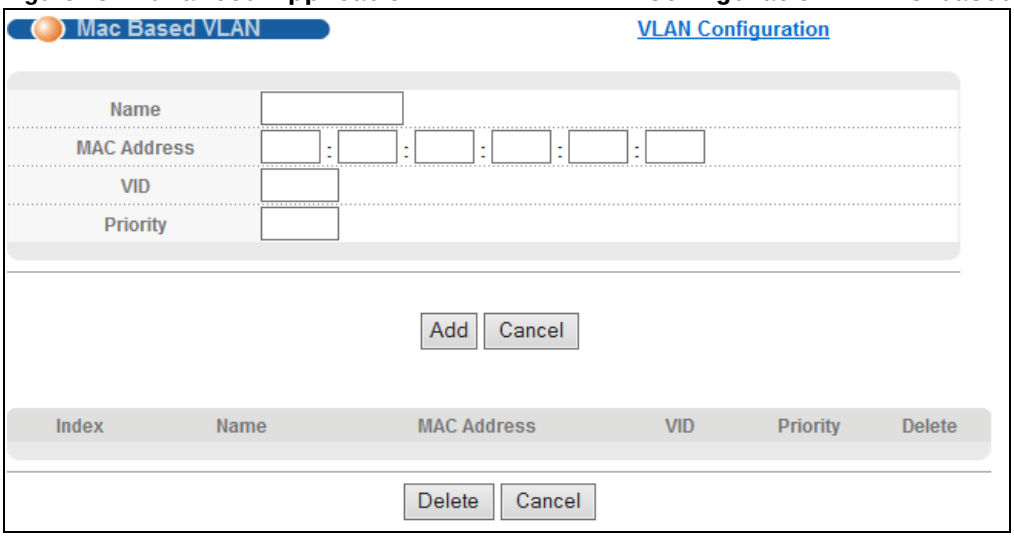
9.10 MAC-based VLAN

The MAC-based VLAN feature assigns incoming untagged packets to a VLAN and classifies the traffic based on the source MAC address of the packet. When untagged packets arrive at the switch, the source MAC address of the packet is looked up in a MAC to VLAN mapping table. If an entry is found, the corresponding VLAN ID is assigned to the packet. The assigned VLAN ID is verified against the VLAN table. If the VLAN is valid, ingress processing on the packet continues; otherwise, the packet is dropped.

This feature allows users to change ports without having to reconfigure the VLAN, which allows better mobility. You can assign priority to the MAC-based VLAN and define a MAC to VLAN mapping table by entering a specified source MAC address in the MAC-based VLAN setup screen. You can also delete a MAC-based VLAN entry in the same screen.

Click **MAC-based VLAN** in the **VLAN Configuration** window to see the following screen.

Figure 73 Advanced Application > VLAN > VLAN Configuration > MAC-based VLAN Setup



The following table describes the fields in the above screen.

Table 41 Advanced Application > VLAN > VLAN Configuration > MAC-based VLAN Setup

LABEL	DESCRIPTION
Name	Type a name up to 32 alpha numeric characters for the MAC-based VLAN entry.
MAC Address	Type a MAC address that is bind to the MAC-based VLAN entry. This is the source MAC address of the data packet that is looked up when untagged packets arrive at the Switch.
VID	Type an ID (from 1 to 4094) for the VLAN ID that is associated with the MAC-based VLAN entry.
Priority	Type a priority (0-7) for the MAC-based VLAN entry.The higher the numeric value you assign, the higher the priority for this MAC-based VLAN entry.
Add	Click **Add** to save the new MAC-based VLAN entry.
Cancel	Click **Cancel** to clear the fields in the MAC-based VLAN entry.
Index	This field displays the index number of the MAC-based VLAN entry.
Name	This field displays the name of the MAC-based VLAN entry.
MAC Address	This field displays the source MAC address that is bind to the MAC-based VLAN entry.
VID	This field displays the VLAN ID of the MAC-based VLAN entry.
Priority	This field displays the priority level of the MAC-based VLAN entry.
Delete	Click the **Delete** check box to select MAC-based VLAN entry you wish to remove.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

9.11 Port-based VLAN Setup

Port-based VLANs are VLANs where the packet forwarding decision is based on the destination MAC address and its associated port.

Port-based VLANs require allowed outgoing ports to be defined for each port. Therefore, if you wish to allow two subscriber ports to talk to each other, for example, between conference rooms in a hotel, you must define the egress (an egress port is an outgoing port, that is, a port through which a data packet leaves) for both ports.

Port-based VLANs are specific only to the Switch on which they were created.

Note: When you activate port-based VLAN, the Switch uses a default VLAN ID of 1. You cannot change it.

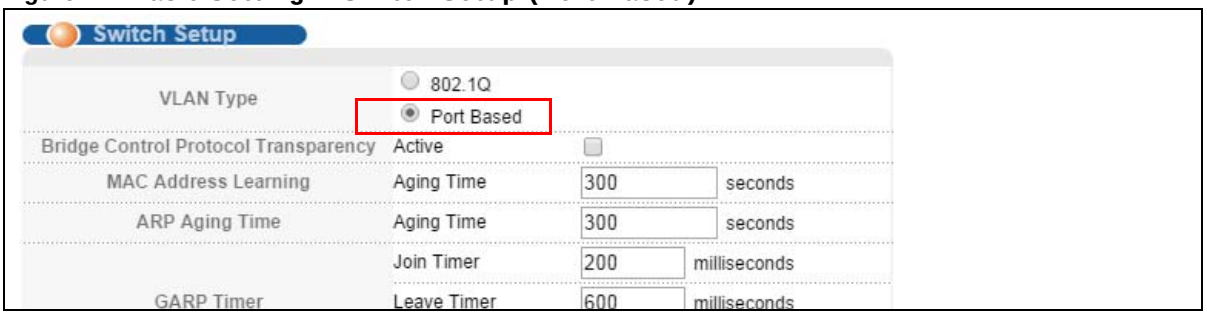
Note: In screens (such as **IP Setup** and **Filtering**) that require a VID, you must enter 1 as the VID.

The port-based VLAN setup screen is shown next. The **CPU** management port forms a VLAN with all Ethernet ports.

9.12 Port-based VLAN

Select **Port Based** as the **VLAN Type** in the **Basic Setting** > **Switch Setup** screen.

Figure 74 Basic Setting > Switch Setup (Port Based)



Then click **Advanced Application** > **VLAN** from the navigation panel to display the next screen.

Figure 75 Port Based VLAN Setup (All Connected)

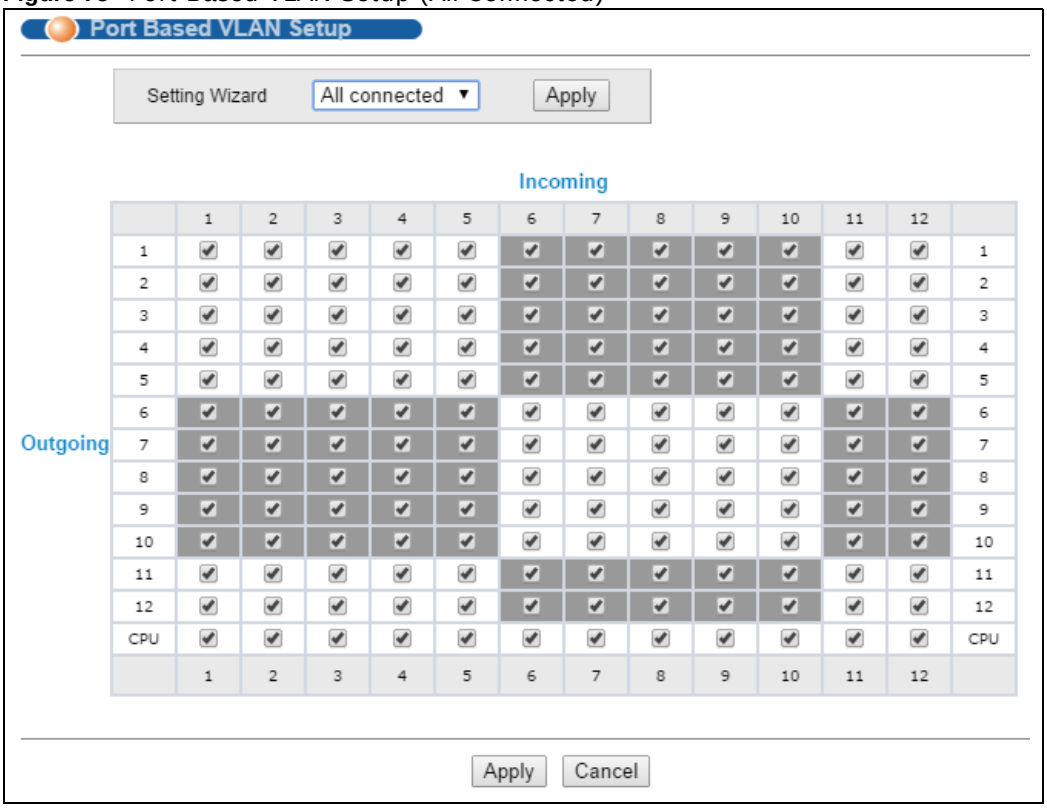
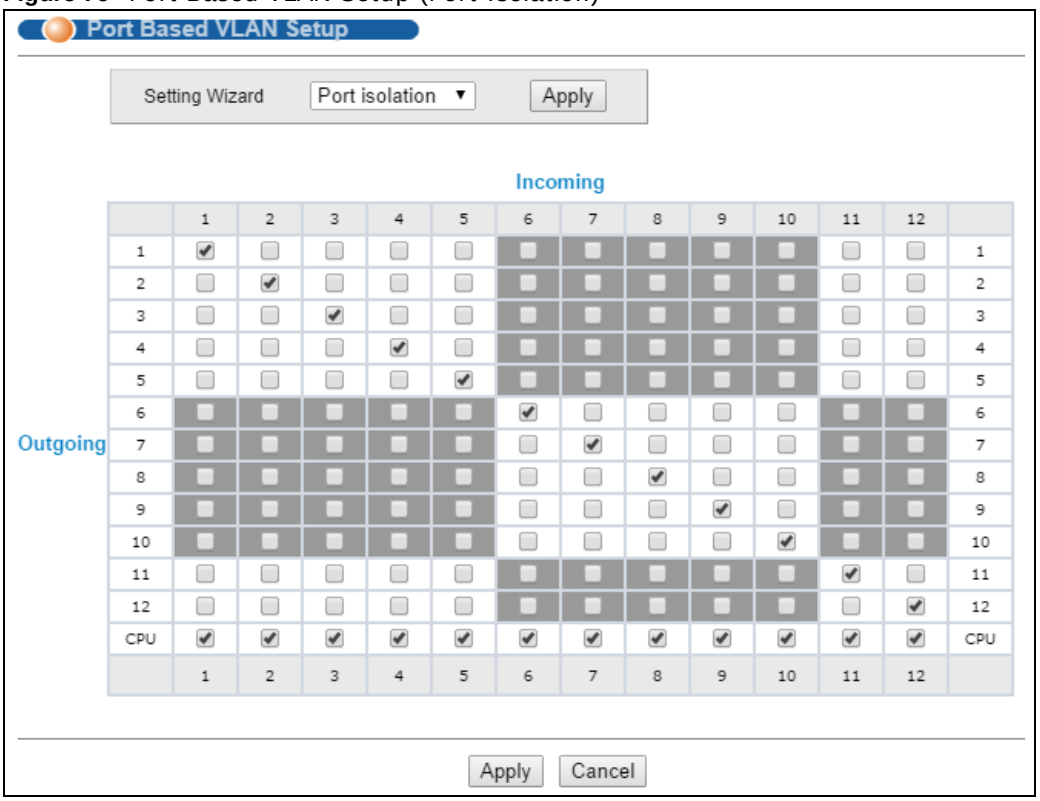


Figure 76 Port Based VLAN Setup (Port Isolation)



The following table describes the labels in this screen.

Table 42 Port Based VLAN Setup

label	Description
Setting Wizard	Choose **All connected** or **Port isolation**. **All connected** means all ports can communicate with each other, that is, there are no virtual LANs. All incoming and outgoing ports are selected. This option is the most flexible but also the least secure. **Port isolation** means that each port can only communicate with the CPU management port and cannot communicate with each other. All incoming ports are selected while only the CPU outgoing port is selected. This option is the most limiting but also the most secure. After you make your selection, click **Apply** (top right of screen) to display the screens as mentioned above. You can still customize these settings by adding/deleting incoming or outgoing ports, but you must also click **Apply** at the bottom of the screen.
Incoming	These are the ingress ports; an ingress port is an incoming port, that is, a port through which a data packet enters. If you wish to allow two subscriber ports to talk to each other, you must define the ingress port for both ports. The numbers in the top row denote the incoming port for the corresponding port listed on the left (its outgoing port). **CPU** refers to the Switch management port. By default it forms a VLAN with all Ethernet ports. If it does not form a VLAN with a particular port then the Switch cannot be managed from that port.
Outgoing	These are the egress ports; an egress port is an outgoing port, that is, a port through which a data packet leaves. If you wish to allow two subscriber ports to talk to each other, you must define the egress port for both ports. **CPU** refers to the Switch management port. By default it forms a VLAN with all Ethernet ports. If it does not form a VLAN with a particular port then the Switch cannot be managed from that port.

Table 42 Port Based VLAN Setup (continued)

label	Description
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

9.13 Technical Reference

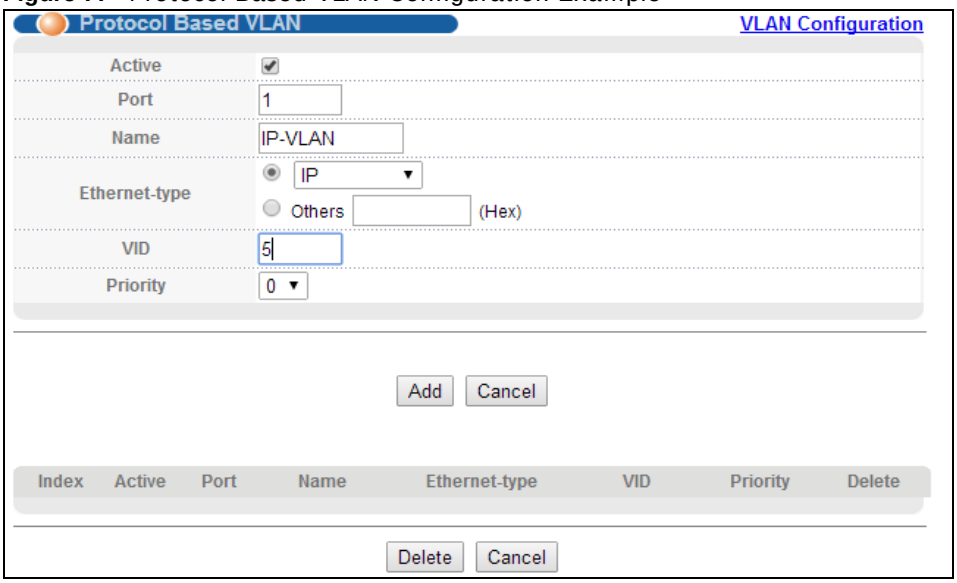
This section provides technical background information on the topics discussed in this chapter.

9.13.1 Create an IP-based VLAN Example

This example shows you how to create an IP VLAN which includes ports 1, 4 and 8. Follow these steps:

1. Activate this protocol based VLAN.
2. Type the port number you want to include in this protocol based VLAN. Type **1**.
3. Give this protocol-based VLAN a descriptive name. Type **IP-VLAN**.
4. Select the protocol. Leave the default value **IP**.
5. Type the VLAN ID of an existing VLAN. In our example we already created a static VLAN with an ID of 5. Type **5**.
6. Leave the priority set to **0** and click **Add**.

Figure 77 Protocol Based VLAN Configuration Example



To add more ports to this protocol based VLAN.

1 Click the index number of the protocol based VLAN entry. Click **1**

2 Change the value in the **Port** field to the next port you want to add.

3 Click **Add**.

10

Static MAC Forward Setup

10.1 Overview

This chapter discusses how to configure forwarding rules based on MAC addresses of devices on your network.

Use these screens to configure static MAC address forwarding.

10.1.1 What You Can Do

Use the **Static MAC Forwarding** screen (Section 10.2 on page 108) to assign static MAC addresses for a port.

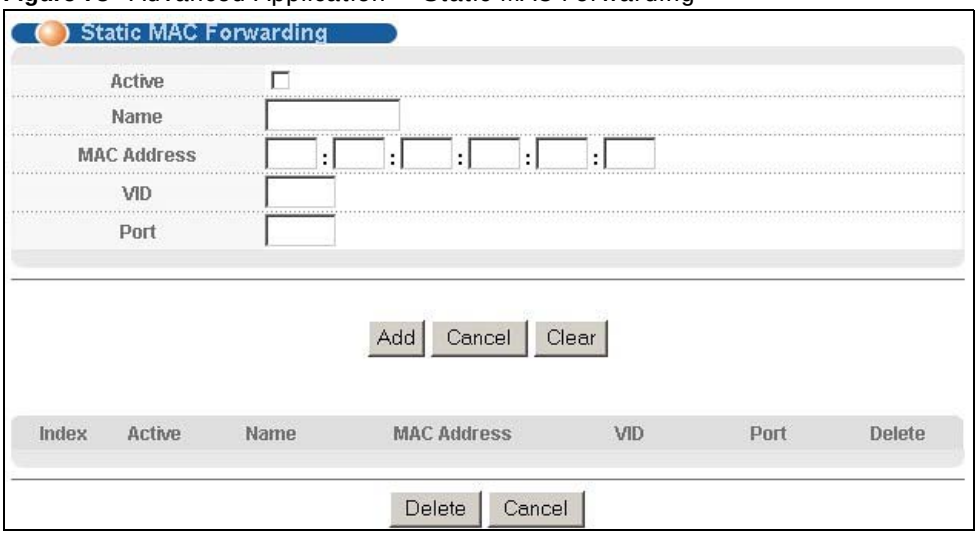
10.2 Configuring Static MAC Forwarding

A static MAC address is an address that has been manually entered in the MAC address table. Static MAC addresses do not age out. When you set up static MAC address rules, you are setting static MAC addresses for a port. This may reduce the need for broadcasting.

Static MAC address forwarding together with port security allow only computers in the MAC address table on a port to access the Switch. See Chapter 19 on page 156 for more information on port security.

Click **Advanced Application** > **Static MAC Forwarding** in the navigation panel to display the configuration screen as shown.

Figure 78 Advanced Application > Static MAC Forwarding



The following table describes the labels in this screen.

Table 43 Advanced Application > Static MAC Forwarding

LABEL	DESCRIPTION
Active	Select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by clearing this check box.
Name	Enter a descriptive name for identification purposes for this static MAC address forwarding rule.
MAC Address	Enter the MAC address in valid MAC address format, that is, six hexadecimal character pairs. Note: Static MAC addresses do not age out.
VID	Enter the VLAN identification number.
Port	Enter the port where the MAC address entered in the previous field will be automatically forwarded.
Add	Click **Add** to save your rule to the Switch's run-time memory. The Switch loses this rule if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to their last saved values.
Clear	Click **Clear** to begin configuring this screen afresh.
Index	Click an index number to modify a static MAC address rule for a port.
Active	This field displays whether this static MAC address forwarding rule is active (**Yes**) or not (**No**). You may temporarily deactivate a rule without deleting it.
Name	This field displays the descriptive name for identification purposes for this static MAC address-forwarding rule.
MAC Address	This field displays the MAC address that will be forwarded and the VLAN identification number to which the MAC address belongs.
VID	This field displays the ID number of the VLAN group.
Port	This field displays the port where the MAC address shown in the next field will be forwarded.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

11

Static Multicast Forward Setup

11.1 Static Multicast Forward Setup Overview

This chapter discusses how to configure forwarding rules based on multicast MAC addresses of devices on your network.

Use these screens to configure static multicast address forwarding.

11.1.1 What You Can Do

Use the **Static Multicast Forward Setup** screen (Section 11.2 on page 111) to configure rules to forward specific multicast frames, such as streaming or control frames, to specific port(s).

11.1.2 What You Need To Know

A multicast MAC address is the MAC address of a member of a multicast group. A static multicast address is a multicast MAC address that has been manually entered in the multicast table. Static multicast addresses do not age out. Static multicast forwarding allows you (the administrator) to forward multicast frames to a member without the member having to join the group first.

If a multicast group has no members, then the switch will either flood the multicast frames to all ports or drop them. Figure 79 shows such unknown multicast frames flooded to all ports. With static multicast forwarding, you can forward these multicasts to port(s) within a VLAN group. Figure 80 shows frames being forwarded to devices connected to port 3. Figure 81 shows frames being forwarded to ports 2 and 3 within VLAN group 4.

Figure 79 No Static Multicast Forwarding

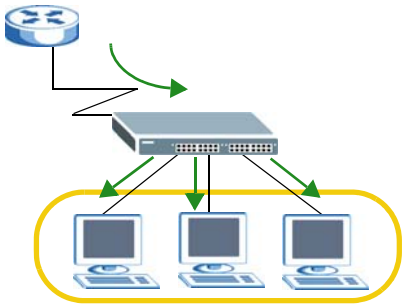


Figure 80 Static Multicast Forwarding to A Single Port

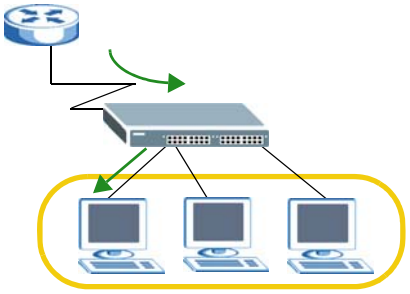
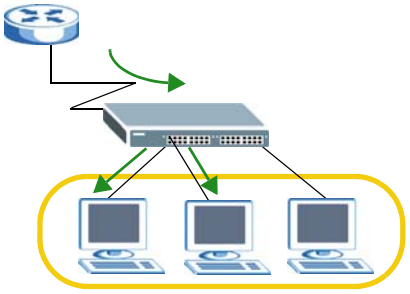


Figure 81 Static Multicast Forwarding to Multiple Ports

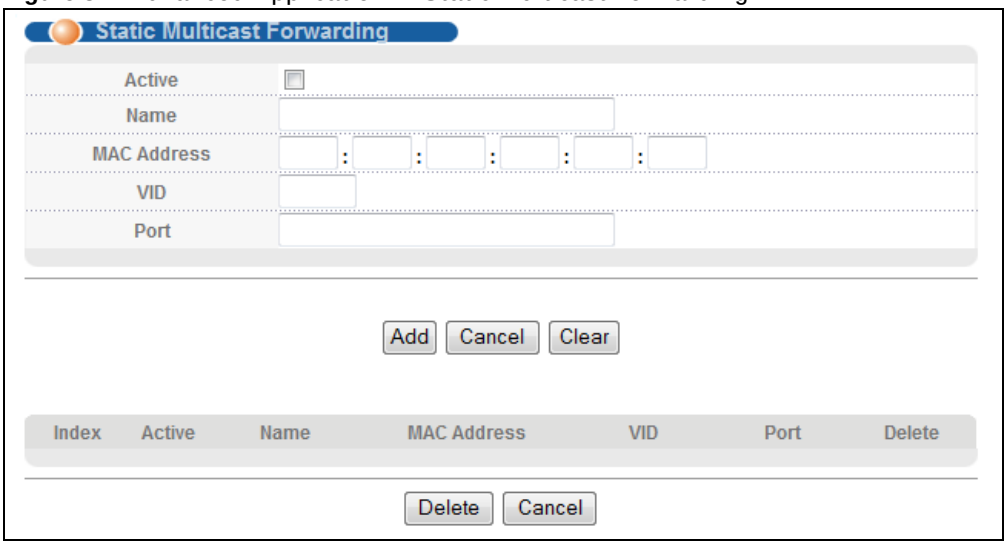


11.2 Configuring Static Multicast Forwarding

Use this screen to configure rules to forward specific multicast frames, such as streaming or control frames, to specific port(s).

Click **Advanced Application** > **Static Multicast Forwarding** to display the configuration screen as shown.

Figure 82 Advanced Application > Static Multicast Forwarding



The following table describes the labels in this screen.

Table 44 Advanced Application > Static Multicast Forwarding

LABEL	DESCRIPTION
Active	Select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by clearing this check box.
Name	Type a descriptive name (up to 32 printable ASCII characters) for this static multicast MAC address forwarding rule. This is for identification only.
MAC Address	Enter a multicast MAC address which identifies the multicast group. The last binary bit of the first octet pair in a multicast MAC address must be 1. For example, the first octet pair 00000001 is 01 and 00000011 is 03 in hexadecimal, so 01:00:5e:00:00:0A and 03:00:5e:00:00:27 are valid multicast MAC addresses.
VID	You can forward frames with matching destination MAC address to port(s) within a VLAN group. Enter the ID that identifies the VLAN group here. If you don't have a specific target VLAN, enter 1.
Port	Enter the port(s) where frames with destination MAC address that matched the entry above are forwarded. You can enter multiple ports separated by (no space) comma (,) or hyphen (-). For example, enter "3-5" for ports 3, 4, and 5. Enter "3,5,7" for ports 3, 5, and 7.
Add	Click **Add** to save your rule to the Switch's run-time memory. The Switch loses this rule if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to their last saved values.
Clear	Click **Clear** to begin configuring this screen afresh.
Index	Click an index number to modify a static multicast MAC address rule for port(s).
Active	This field displays whether a static multicast MAC address forwarding rule is active (**Yes**) or not (**No**). You may temporarily deactivate a rule without deleting it.
Name	This field displays the descriptive name for identification purposes for a static multicast MAC address-forwarding rule.
MAC Address	This field displays the multicast MAC address that identifies a multicast group.
VID	This field displays the ID number of a VLAN group to which frames containing the specified multicast MAC address will be forwarded.
Port	This field displays the port(s) within a identified VLAN group to which frames containing the specified multicast MAC address will be forwarded.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

12 Filtering

12.1 Filtering Overview

This chapter discusses MAC address port filtering.

Filtering means sifting traffic going through the Switch based on the source and/or destination MAC addresses and VLAN group (ID).

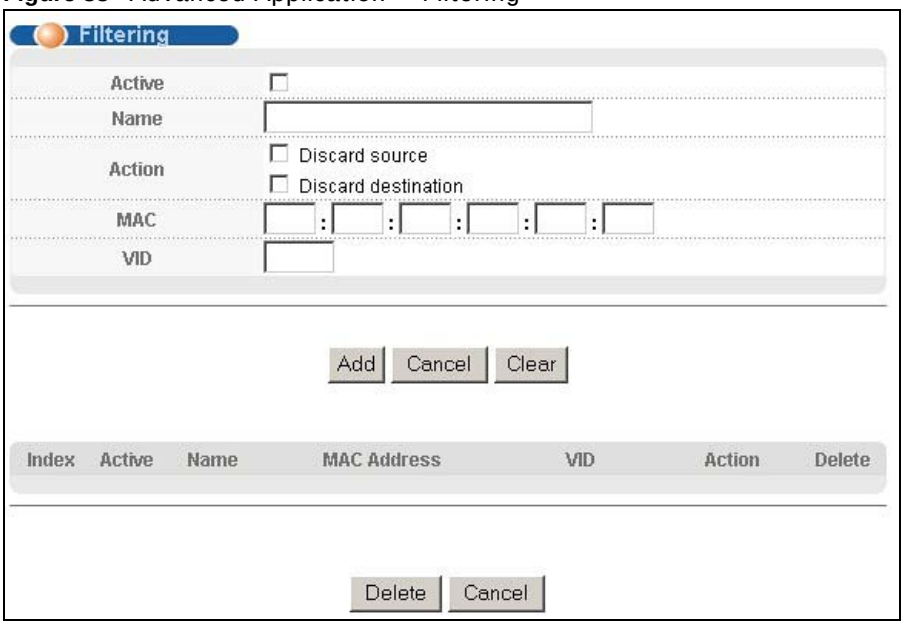
12.1.1 What You Can Do

Use the **Filtering** screen (Section 12.2 on page 113) to create rules for traffic going through the Switch.

12.2 Configure a Filtering Rule

Use this screen to create rules for traffic going through the Switch. Click **Advanced Application** > **Filtering** in the navigation panel to display the screen as shown next.

Figure 83 Advanced Application > Filtering



The following table describes the related labels in this screen.

Table 45 Advanced Application > Filtering

LABEL	DESCRIPTION
Active	Make sure to select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by deselecting this check box.
Name	Type a descriptive name (up to 32 printable ASCII characters) for this rule. This is for identification only.
Action	Select **Discard source** to drop the frames from the source MAC address (specified in the **MAC** field). The Switch can still send frames to the MAC address. Select **Discard destination** to drop the frames to the destination MAC address (specified in the **MAC** address). The Switch can still receive frames originating from the MAC address. Select **Discard source** and **Discard destination** to block traffic to/from the MAC address specified in the **MAC** field.
MAC	Type a MAC address in valid MAC address format, that is, six hexadecimal character pairs.
VID	Type the VLAN group identification number.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to your previous configuration.
Clear	Click **Clear** to clear the fields to the factory defaults.
Index	This field displays the index number of the rule. Click an index number to change the settings.
Active	This field displays **Yes** when the rule is activated and **No** when is it deactivated.
Name	This field displays the descriptive name for this rule. This is for identification purpose only.
MAC Address	This field displays the source/destination MAC address with the VLAN identification number to which the MAC address belongs.
VID	This field displays the VLAN group identification number.
Delete	Check the rule(s) that you want to remove in the **Delete** column and then click the **Delete** button.
Cancel	Click **Cancel** to clear the selected checkbox(es) in the **Delete** column.

13

Spanning Tree Protocol

13.1 Spanning Tree Protocol Overview

The Switch supports Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP) as defined in the following standards.

- IEEE 802.1D Spanning Tree Protocol
- IEEE 802.1w Rapid Spanning Tree Protocol
- IEEE 802.1s Multiple Spanning Tree Protocol

The Switch also allows you to set up multiple STP configurations (or trees). Ports can then be assigned to the trees.

13.1.1 What You Can Do

- Use the **Spanning Tree Protocol** status screen (Section 13.2 on page 118) to view the STP status in the different STP modes (RSTP, MRSTP or MSTP) you can configure on the Switch.
- Use the **Spanning Tree Configuration** screen (Section 13.3 on page 118) to activate one of the STP modes on the Switch.
- Use the **Rapid Spanning Tree Protocol** screen (Section 13.4 on page 119) to configure RSTP settings.
- Use the **Rapid Spanning Tree Protocol Status** screen (Section 13.4.1 on page 121) to display the status screen as shown next.
- Use the **Multiple Rapid Spanning Tree Protocol** screen (Section 13.5 on page 122) to configure MRSTP.
- Use the **Multiple Rapid Spanning Tree Protocol Status** screen (Section 13.5.1 on page 124) to view the MRSTP status.
- Use the **Multiple Spanning Tree Protocol** screen (Section 13.6 on page 125) to configure MSTP.
- Use the **Multiple Spanning Tree Protocol Status** screen (Section 13.6.2 on page 129) to view the MSTP status.

13.1.2 What You Need to Know

Read on for concepts on STP that can help you configure the screens in this chapter.

(Rapid) Spanning Tree Protocol

(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a switch to interact with other (R)STP -compliant switches in your network to ensure that only one path exists between any two stations on the network.

The Switch uses IEEE 802.1w RSTP (Rapid Spanning Tree Protocol) that allows faster convergence of the spanning tree than STP (while also being backwards compatible with STP-only aware bridges). In RSTP, topology change information is directly propagated throughout the network from the device that generates the topology change. In STP, a longer delay is required as the device that causes a topology change first notifies the root bridge that then notifies the network. Both RSTP and STP flush unwanted learned addresses from the filtering database. In RSTP, the port states are Discarding, Learning, and Forwarding.

Note: In this user's guide, "STP" refers to both STP and RSTP.

STP Terminology

The root bridge is the base of the spanning tree.

Path cost is the cost of transmitting a frame onto a LAN through that port. The recommended cost is assigned according to the speed of the link to which a port is attached. The slower the media, the higher the cost.

Table 46 STP Path Costs

	LINK SPEED	RECOMMENDED VALUE	RECOMMENDED RANGE	ALLOWED RANGE
Path Cost	4Mbps	250	100 to 1000	1 to 65535
Path Cost	10Mbps	100	50 to 600	1 to 65535
Path Cost	16Mbps	62	40 to 400	1 to 65535
Path Cost	100Mbps	19	10 to 60	1 to 65535
Path Cost	1Gbps	4	3 to 10	1 to 65535
Path Cost	10Gbps	2	1 to 5	1 to 65535

On each bridge, the root port is the port through which this bridge communicates with the root. It is the port on this switch with the lowest path cost to the root (the root path cost). If there is no root port, then this switch has been accepted as the root bridge of the spanning tree network.

For each LAN segment, a designated bridge is selected. This bridge has the lowest cost to the root among the bridges connected to the LAN.

How STP Works

After a bridge determines the lowest cost-spanning tree with STP, it enables the root port and the ports that are the designated ports for connected LANs, and disables all other ports that participate in STP. Network packets are therefore only forwarded between enabled ports, eliminating any possible network loops.

STP-aware switches exchange Bridge Protocol Data Units (BPDUs) periodically. When the bridged LAN topology changes, a new spanning tree is constructed.

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (Max Age), the bridge assumes that the link to the root bridge is down. This bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology.

STP Port States

STP assigns five port states to eliminate packet looping. A bridge port is not allowed to go directly from blocking state to forwarding state so as to eliminate transient loops.

Table 47 STP Port States

PORT STATE	DESCRIPTION
Disabled	STP is disabled (default).
Blocking	Only configuration and management BPDUs are received and processed.
Listening	All BPDUs are received and processed. Note: The listening state does not exist in RSTP.
Learning	All BPDUs are received and processed. Information frames are submitted to the learning process but not forwarded.
Forwarding	All BPDUs are received and processed. All information frames are received and forwarded.

Multiple RSTP

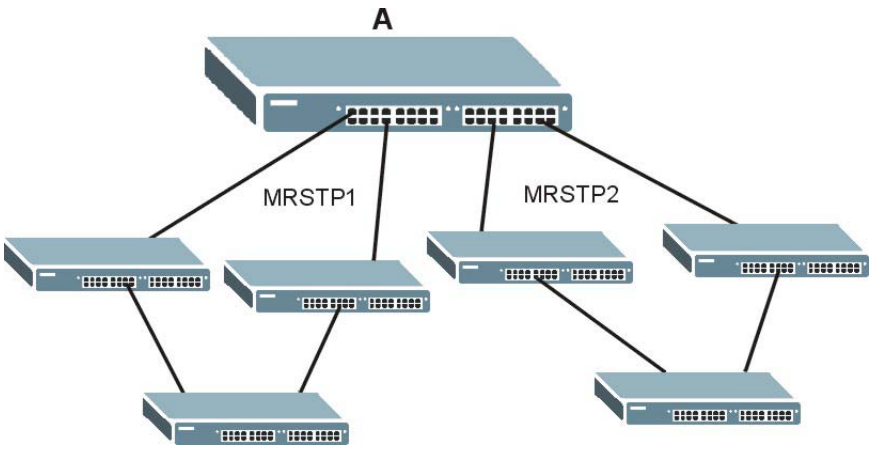
MRSTP (Multiple RSTP) is ZyXEL's proprietary feature that is compatible with RSTP and STP. With MRSTP, you can have more than one spanning tree on your Switch and assign port(s) to each tree. Each spanning tree operates independently with its own bridge information.

In the following example, there are two RSTP instances (**MRSTP 1** and **MRSTP2**) on switch **A**.

To set up MRSTP, activate MRSTP on the Switch and specify which port(s) belong to which spanning tree.

Note: Each port can belong to one STP tree only.

Figure 84 MRSTP Network Example



Multiple STP

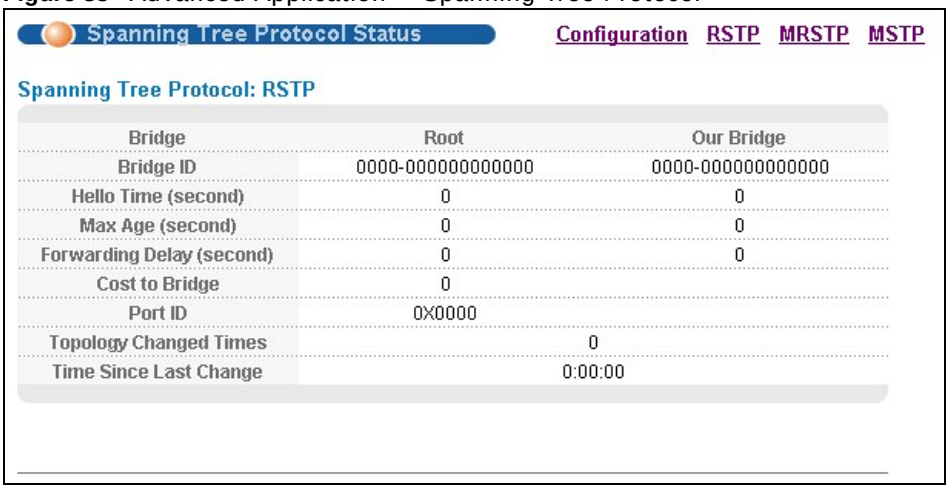
Multiple Spanning Tree Protocol (IEEE 802.1s) is backward compatible with STP/RSTP and addresses the limitations of existing spanning tree protocols (STP and RSTP) in networks to include the following features:

- One Common and Internal Spanning Tree (CIST) that represents the entire network's connectivity.
- Grouping of multiple bridges (or switching devices) into regions that appear as one single bridge on the network.
- A VLAN can be mapped to a specific Multiple Spanning Tree Instance (MSTI). MSTI allows multiple VLANs to use the same spanning tree.
- Load-balancing is possible as traffic from different VLANs can use distinct paths in a region.

13.2 Spanning Tree Protocol Status Screen

The Spanning Tree Protocol status screen changes depending on what standard you choose to implement on your network. Click **Advanced Application** > **Spanning Tree Protocol** to see the screen as shown.

Figure 85 Advanced Application > Spanning Tree Protocol

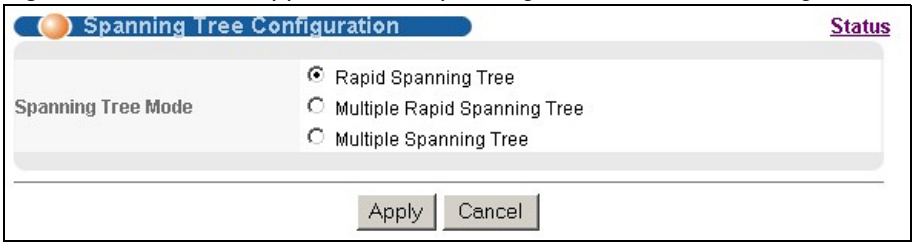


This screen differs depending on which STP mode (RSTP, MRSTP or MSTP) you configure on the Switch. This screen is described in detail in the section that follows the configuration section for each STP mode. Click **Configuration** to activate one of the STP standards on the Switch.

13.3 Spanning Tree Configuration

Use the **Spanning Tree Configuration** screen to activate one of the STP modes on the Switch. Click **Configuration** in the **Advanced Application** > **Spanning Tree Protocol**.

Figure 86 Advanced Application > Spanning Tree Protocol > Configuration



The following table describes the labels in this screen.

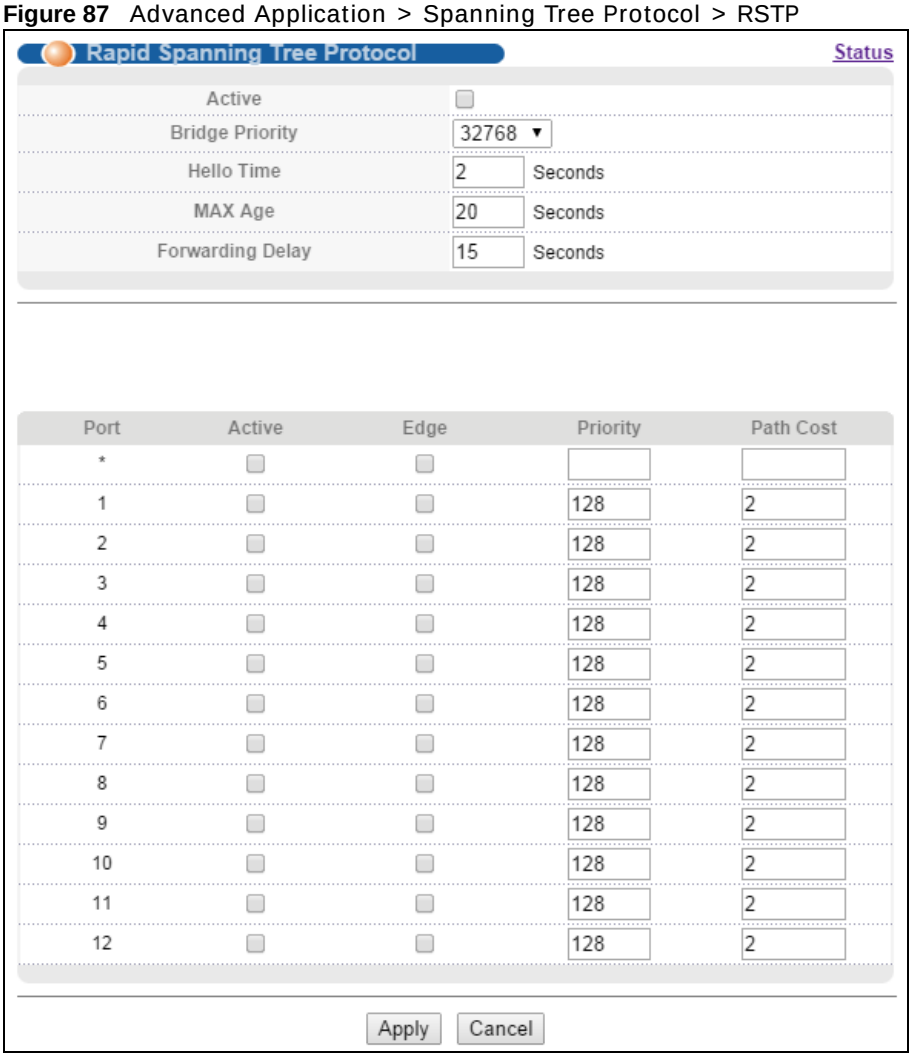
Table 48 Advanced Application > Spanning Tree Protocol > Configuration

LABEL	DESCRIPTION
Spanning Tree Mode	You can activate one of the STP modes on the Switch. Select **Rapid Spanning Tree**, **Multiple Rapid Spanning Tree** or **Multiple Spanning Tree**. See Section 13.1 on page 115 for background information on STP.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

13.4 Configure Rapid Spanning Tree Protocol

Use this screen to configure RSTP settings, see Section 13.1 on page 115 for more information on RSTP. Click **RSTP** in the **Advanced Application** > **Spanning Tree Protocol** screen.

Figure 87 Advanced Application > Spanning Tree Protocol > RSTP



The following table describes the labels in this screen.

Table 49 Advanced Application > Spanning Tree Protocol > RSTP

LABEL	DESCRIPTION
Status	Click **Status** to display the **RSTP Status** screen (see Figure 88 on page 121).
Active	Select this check box to activate RSTP. Clear this checkbox to disable RSTP. Note: You must also activate **Rapid Spanning Tree** in the **Advanced Application > Spanning Tree Protocol > Configuration** screen to enable RSTP on the Switch.
Bridge Priority	Bridge priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch. Select a value from the drop-down list box. The lower the numeric value you assign, the higher the priority for this bridge. Bridge Priority determines the root bridge, which in turn determines Hello Time, Max Age and Forwarding Delay.
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.
Max Age	This is the maximum time (in seconds) the Switch can wait without receiving a BPDU before attempting to reconfigure. All Switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the Switch ports attached to the network. The allowed range is 6 to 40 seconds.
Forwarding Delay	This is the maximum time (in seconds) the Switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds. As a general rule: Note: 2 * (Forward Delay - 1) >= Max Age >= 2 * (Hello Time + 1)
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to activate RSTP on this port.
Edge	Select this check box to configure a port as an edge port when it is directly attached to a computer. An edge port changes its initial STP port state from blocking state to forwarding state immediately without going through listening and learning states right after the port is configured as an edge port or when its link status changes. Note: An edge port becomes a non-edge port as soon as it receives a Bridge Protocol Data Unit (BPDU).
Priority	Configure the priority for each port here. Priority decides which port should be disabled when more than one port forms a loop in a switch. Ports with a higher priority numeric value are disabled first. The allowed range is between 0 and 255 and the default value is 128.

Table 49 Advanced Application > Spanning Tree Protocol > RSTP (continued)

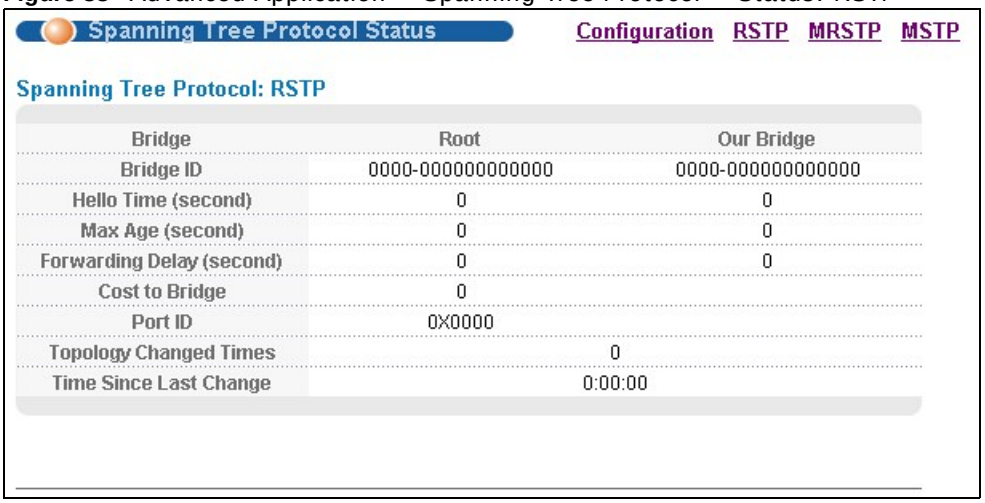
LABEL	DESCRIPTION
Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost-see Table 46 on page 116 for more information.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

13.4.1 Rapid Spanning Tree Protocol Status

Click **Advanced Application** > **Spanning Tree Protocol** in the navigation panel to display the status screen as shown next. See Section 13.1 on page 115 for more information on RSTP.

Note: This screen is only available after you activate RSTP on the Switch.

Figure 88 Advanced Application > Spanning Tree Protocol > Status: RSTP



The following table describes the labels in this screen.

Table 50 Advanced Application > Spanning Tree Protocol > Status: RSTP

LABEL	DESCRIPTION
Configuration	Click **Configuration** to specify which STP mode you want to activate. Click **RSTP** to edit RSTP settings on the Switch.
Bridge	**Root** refers to the base of the spanning tree (the root bridge). **Our Bridge** is this switch. This Switch may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address. This ID is the same for **Root** and **Our Bridge** if the Switch is the root switch.
Hello Time (second)	This is the time interval (in seconds) at which the root switch transmits a configuration message. The root bridge determines Hello Time, Max Age and Forwarding Delay.
Max Age (second)	This is the maximum time (in seconds) the Switch can wait without receiving a configuration message before attempting to reconfigure.

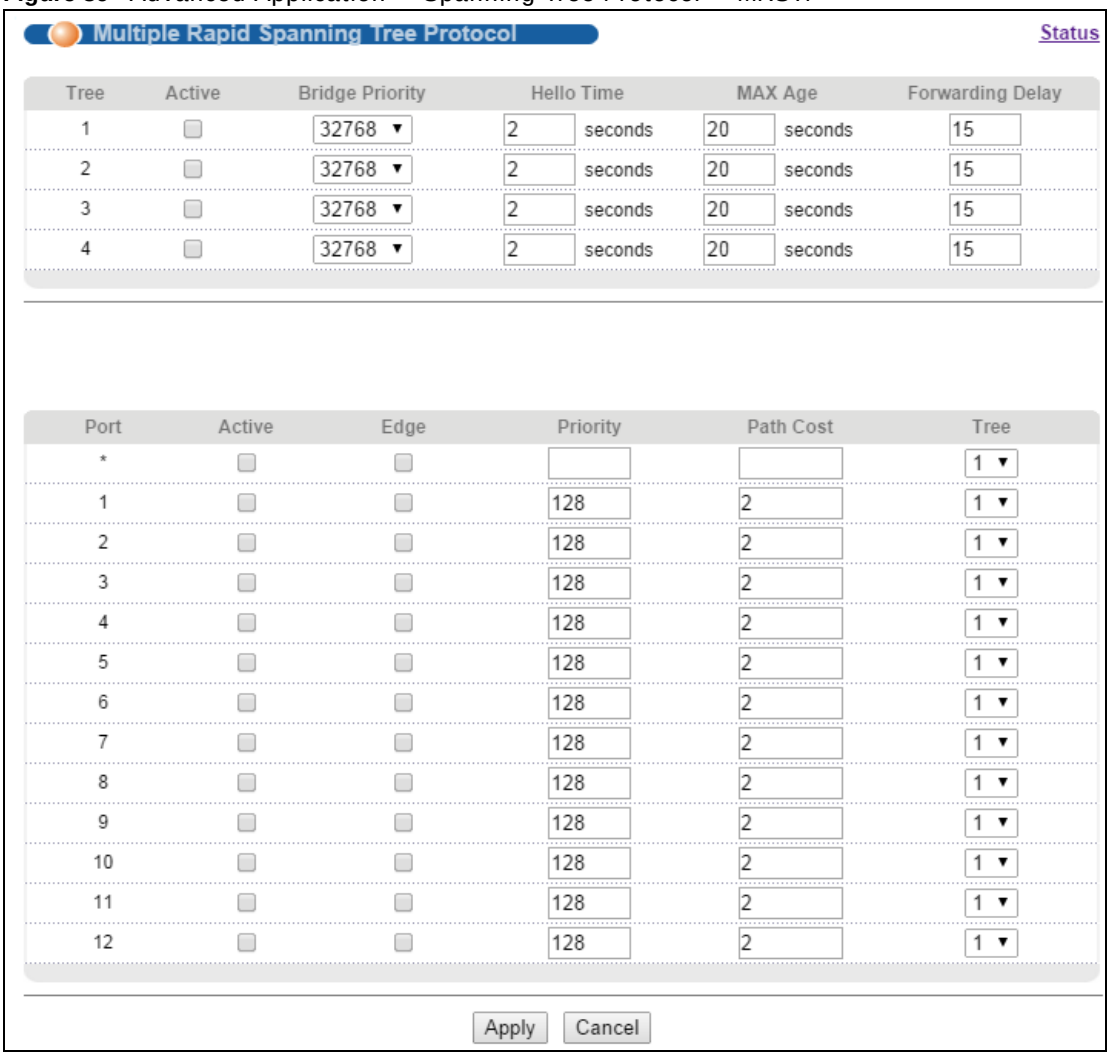
Table 50 Advanced Application > Spanning Tree Protocol > Status: RSTP (continued)

LABEL	DESCRIPTION
Forwarding Delay (second)	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding). Note: The listening state does not exist in RSTP.
Cost to Bridge	This is the path cost from the root port on this Switch to the root switch.
Port ID	This is the priority and number of the port on the Switch through which this Switch must communicate with the root of the Spanning Tree.
Topology Changed Times	This is the number of times the spanning tree has been reconfigured.
Time Since Last Change	This is the time since the spanning tree was last reconfigured.

13.5 Configure Multiple Rapid Spanning Tree Protocol

To configure MRSTP, click **MRSTP** in the **Advanced Application** > **Spanning Tree Protocol** screen. See Section 13.1 on page 115 for more information on MRSTP.

Figure 89 Advanced Application > Spanning Tree Protocol > MRSTP



The following table describes the labels in this screen.

Table 51 Advanced Application > Spanning Tree Protocol > MRSTP

LABEL	DESCRIPTION
Status	Click **Status** to display the **MRSTP Status** screen (see Figure 88 on page 121).
Tree	This is a read only index number of the STP trees.
Active	Select this check box to activate an STP tree. Clear this checkbox to disable an STP tree. Note: You must also activate **Multiple Rapid Spanning Tree** in the **Advanced Application** > **Spanning Tree Protocol** > **Configuration** screen to enable MRSTP on the Switch.
Bridge Priority	Bridge priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch. Select a value from the drop-down list box. The lower the numeric value you assign, the higher the priority for this bridge. Bridge Priority determines the root bridge, which in turn determines Hello Time, Max Age and Forwarding Delay.

Table 51 Advanced Application > Spanning Tree Protocol > MRSTP (continued)

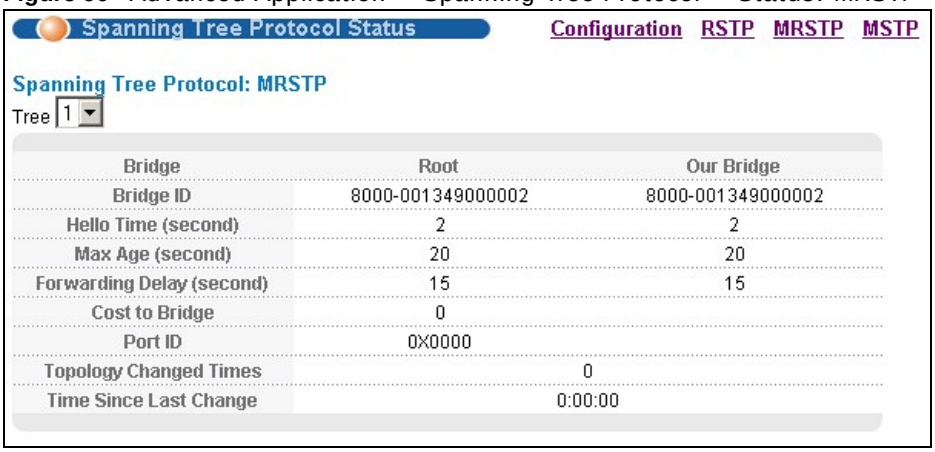
LABEL	DESCRIPTION
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.
Max Age	This is the maximum time (in seconds) the Switch can wait without receiving a BPDU before attempting to reconfigure. All Switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the Switch ports attached to the network. The allowed range is 6 to 40 seconds.
Forwarding Delay	This is the maximum time (in seconds) the Switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds. As a general rule: Note: 2 * (Forward Delay - 1) >= Max Age >= 2 * (Hello Time + 1)
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to activate STP on this port.
Edge	Select this check box to configure a port as an edge port when it is directly attached to a computer. An edge port changes its initial STP port state from blocking state to forwarding state immediately without going through listening and learning states right after the port is configured as an edge port or when its link status changes. Note: An edge port becomes a non-edge port as soon as it receives a Bridge Protocol Data Unit (BPDU).
Priority	Configure the priority for each port here. Priority decides which port should be disabled when more than one port forms a loop in a switch. Ports with a higher priority numeric value are disabled first. The allowed range is between 0 and 255 and the default value is 128.
Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost-see Table 46 on page 116 for more information.
Tree	Select which STP tree configuration this port should participate in.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

13.5.1 Multiple Rapid Spanning Tree Protocol Status

Click **Advanced Application** > **Spanning Tree Protocol** in the navigation panel to display the status screen as shown next. See Section 13.1 on page 115 for more information on MRSTP.

Note: This screen is only available after you activate MRSTP on the Switch.

Figure 90 Advanced Application > Spanning Tree Protocol > Status: MRSTP



The following table describes the labels in this screen.

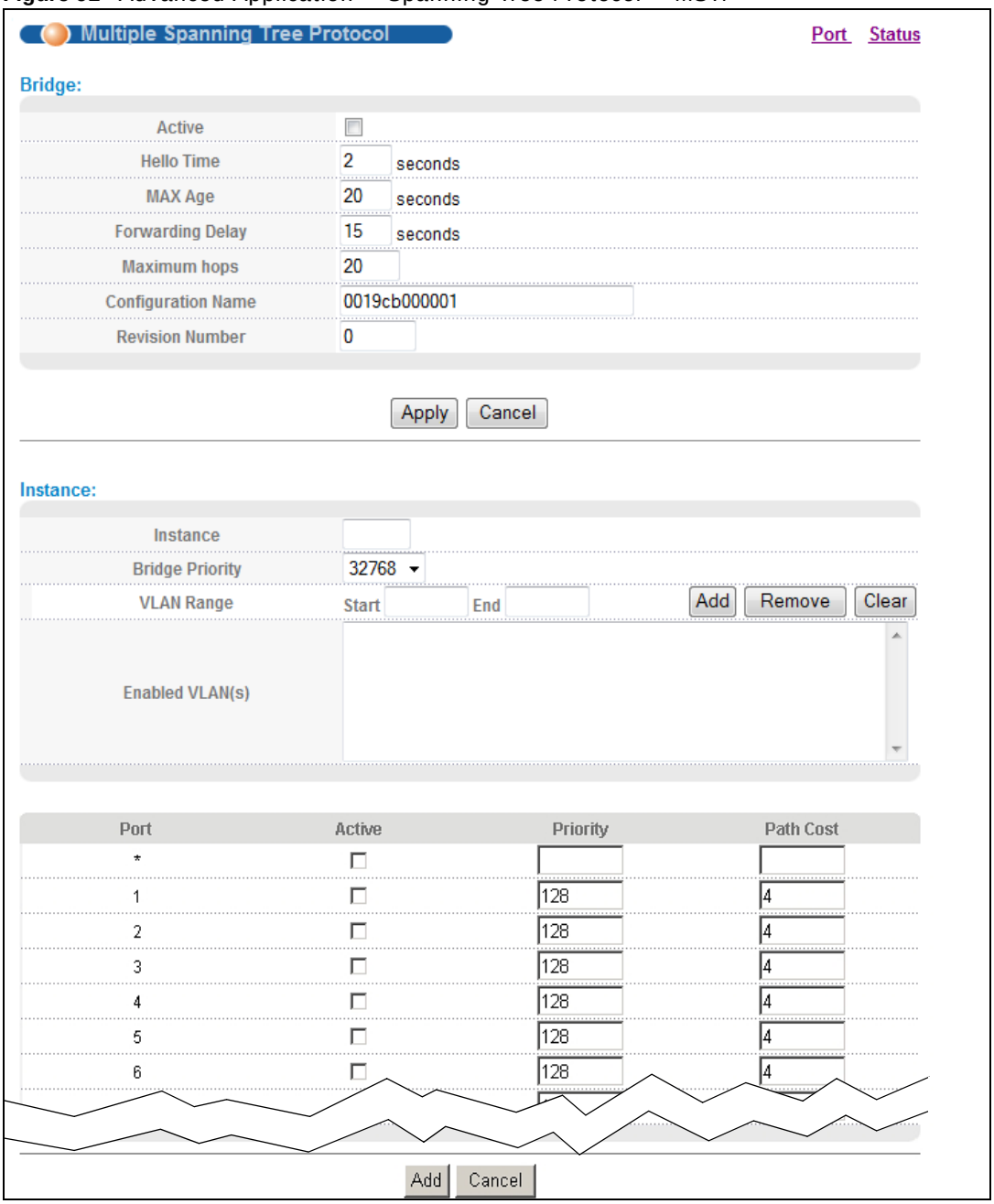
Table 52 Advanced Application > Spanning Tree Protocol > Status: MRSTP

LABEL	DESCRIPTION
Configuration	Click **Configuration** to specify which STP mode you want to activate. Click **MRSTP** to edit MRSTP settings on the Switch.
Tree	Select which STP tree configuration you want to view.
Bridge	**Root** refers to the base of the spanning tree (the root bridge). **Our Bridge** is this switch. This Switch may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address. This ID is the same for **Root** and **Our Bridge** if the Switch is the root switch.
Hello Time (second)	This is the time interval (in seconds) at which the root switch transmits a configuration message. The root bridge determines Hello Time, Max Age and Forwarding Delay.
Max Age (second)	This is the maximum time (in seconds) the Switch can wait without receiving a configuration message before attempting to reconfigure.
Forwarding Delay (second)	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding). Note: The listening state does not exist in RSTP.
Cost to Bridge	This is the path cost from the root port on this Switch to the root switch.
Port ID	This is the priority and number of the port on the Switch through which this Switch must communicate with the root of the Spanning Tree.
Topology Changed Times	This is the number of times the spanning tree has been reconfigured.
Time Since Last Change	This is the time since the spanning tree was last reconfigured.

13.6 Configure Multiple Spanning Tree Protocol

To configure MSTP, click **MSTP** in the **Advanced Application** > **Spanning Tree Protocol** screen. See Section on page 117 for more information on MSTP.

Figure 91 Advanced Application > Spanning Tree Protocol > MSTP



The following table describes the labels in this screen.

Table 53 Advanced Application > Spanning Tree Protocol > MSTP

LABEL	DESCRIPTION
Port	Click **Port** to display the **MSTP Port** screen (see Figure 92 on page 128).
Status	Click **Status** to display the **MSTP Status** screen (see Figure 93 on page 130).
Active	Select this to activate MSTP on the Switch. Clear this to disable MSTP on the Switch. Note: You must also activate **Multiple Spanning Tree** in the **Advanced Application > Spanning Tree Protocol > Configuration** screen to enable MSTP on the Switch.

Table 53 Advanced Application > Spanning Tree Protocol > MSTP (continued)

LABEL	DESCRIPTION
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.
MaxAge	This is the maximum time (in seconds) the Switch can wait without receiving a BPDU before attempting to reconfigure. All Switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the Switch ports attached to the network. The allowed range is 6 to 40 seconds.
Forwarding Delay	This is the maximum time (in seconds) the Switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds. As a general rule: Note: 2 * (Forward Delay - 1) >= Max Age >= 2 * (Hello Time + 1)
Maximum hops	Enter the number of hops (between 1 and 255) in an MSTP region before the BPDU is discarded and the port information is aged.
Configuration Name	Enter a descriptive name (up to 32 characters) of an MST region.
Revision Number	Enter a number to identify a region's configuration. Devices must have the same revision number to belong to the same region.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Instance	Use this section to configure MSTI (Multiple Spanning Tree Instance) settings.
Instance	Enter the number you want to use to identify this MST instance on the Switch. The Switch supports instance numbers 0-15.
Bridge Priority	Set the priority of the Switch for the specific spanning tree instance. The lower the number, the more likely the Switch will be chosen as the root bridge within the spanning tree instance. Enter priority values between 0 and 61440 in increments of 4096 (thus valid values are 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344 and 61440).
VLAN Range	Enter the start of the VLAN ID range that you want to add or remove from the VLAN range edit area in the **Start** field. Enter the end of the VLAN ID range that you want to add or remove from the VLAN range edit area in the **End** field. Next click: • **Add** - to add this range of VLAN(s) to be mapped to the MST instance. • **Remove** - to remove this range of VLAN(s) from being mapped to the MST instance. • **Clear** - to remove all VLAN(s) from being mapped to this MST instance.
Enabled VLAN(s)	This field displays which VLAN(s) are mapped to this MST instance.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.

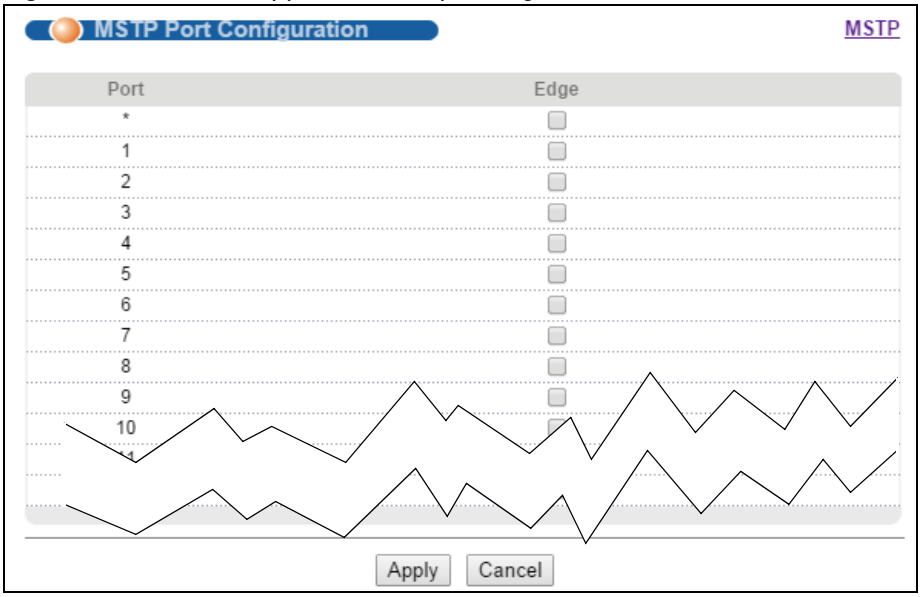
Table 53 Advanced Application > Spanning Tree Protocol > MSTP (continued)

LABEL	DESCRIPTION
Active	Select this check box to add this port to the MST instance.
Priority	Configure the priority for each port here. Priority decides which port should be disabled when more than one port forms a loop in a switch. Ports with a higher priority numeric value are disabled first. The allowed range is between 0 and 255 and the default value is 128.
Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost-see Table 46 on page 116 for more information.
Add	Click **Add** to save this MST instance to the Switch's run-time memory. The Switch loses this change if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Instance	This field displays the ID of an MST instance.
VLAN	This field displays the VID (or VID ranges) to which the MST instance is mapped.
Active Port	This field display the ports configured to participate in the MST instance.
Delete	Check the rule(s) that you want to remove in the **Delete** column and then click the **Delete** button.
Cancel	Click **Cancel** to begin configuring this screen afresh.

13.6.1 Multiple Spanning Tree Port Configuration

Click **Advanced Application** > **Spanning Tree Protocol > MSTP > Port** in the navigation panel to display the status screen as shown next. See Section on page 117 for more information on MSTP.

Figure 92 Advanced Application > Spanning Tree Protocol > MSTP > Port



The following table describes the labels in this screen.

Table 54 Advanced Application > Spanning Tree Protocol > MSTP > Port

LABEL	DESCRIPTION
MSTP	Click **MSTP** to edit MSTP settings on the Switch.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Edge	Select this check box to configure a port as an edge port when it is directly attached to a computer. An edge port changes its initial STP port state from blocking state to forwarding state immediately without going through listening and learning states right after the port is configured as an edge port or when its link status changes. Note: An edge port becomes a non-edge port as soon as it receives a Bridge Protocol Data Unit (BPDU).
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

13.6.2 Multiple Spanning Tree Protocol Status

Click **Advanced Application** > **Spanning Tree Protocol** in the navigation panel to display the status screen as shown next. See Section on page 117 for more information on MSTP.

Note: This screen is only available after you activate MSTP on the Switch.

Figure 93 Advanced Application > Spanning Tree Protocol > Status: MSTP

The following table describes the labels in this screen.

Table 55 Advanced Application > Spanning Tree Protocol > Status: MSTP

LABEL	DESCRIPTION
Configuration	Click **Configuration** to specify which STP mode you want to activate. Click **MSTP** to edit MSTP settings on the Switch.
CST	This section describes the Common Spanning Tree settings.
Bridge	**Root** refers to the base of the spanning tree (the root bridge). **Our Bridge** is this switch. This Switch may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address. This ID is the same for **Root** and **Our Bridge** if the Switch is the root switch.
Hello Time (second)	This is the time interval (in seconds) at which the root switch transmits a configuration message.
Max Age (second)	This is the maximum time (in seconds) the Switch can wait without receiving a configuration message before attempting to reconfigure.
Forwarding Delay (second)	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding).
Cost to Bridge	This is the path cost from the root port on this Switch to the root switch.
Port ID	This is the priority and number of the port on the Switch through which this Switch must communicate with the root of the Spanning Tree.

Table 55 Advanced Application > Spanning Tree Protocol > Status: MSTP (continued)

LABEL	DESCRIPTION
Configuration Name	This field displays the configuration name for this MST region.
Revision Number	This field displays the revision number for this MST region.
Configuration Digest	A configuration digest is generated from the VLAN-MSTI mapping information. This field displays the 16-octet signature that is included in an MSTP BPDU. This field displays the digest when MSTP is activated on the system.
Topology Changed Times	This is the number of times the spanning tree has been reconfigured.
Time Since Last Change	This is the time since the spanning tree was last reconfigured.
Instance:	These fields display the MSTI to VLAN mapping. In other words, which VLANs run on each spanning tree instance.
Instance	This field displays the MSTI ID.
VLAN	This field displays which VLANs are mapped to an MSTI.
MSTI	Select the MST instance settings you want to view.
Bridge	**Root** refers to the base of the MST instance. **Our Bridge** is this switch. This Switch may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address. This ID is the same for **Root** and **Our Bridge** if the Switch is the root switch.
Internal Cost	This is the path cost from the root port in this MST instance to the regional root switch.
Port ID	This is the priority and number of the port on the Switch through which this Switch must communicate with the root of the MST instance.

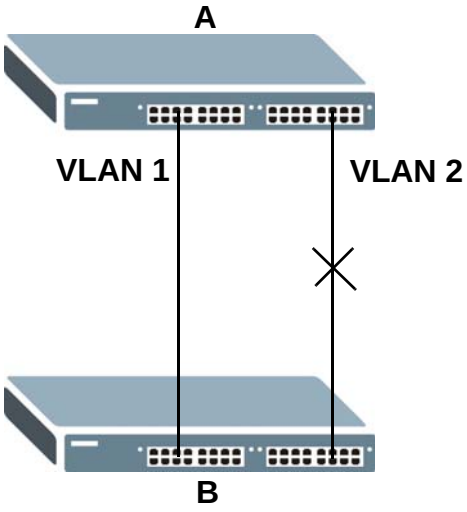
13.7 Technical Reference

This section provides technical background information on the topics discussed in this chapter.

13.7.1 MSTP Network Example

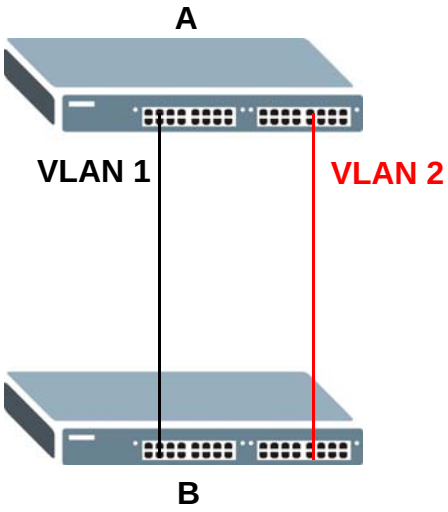
The following figure shows a network example where two VLANs are configured on the two switches. If the switches are using STP or RSTP, the link for VLAN 2 will be blocked as STP and RSTP allow only one link in the network and block the redundant link.

Figure 94 STP/RSTP Network Example



With MSTP, VLANs 1 and 2 are mapped to different spanning trees in the network. Thus traffic from the two VLANs travel on different paths. The following figure shows the network example using MSTP.

Figure 95 MSTP Network Example



13.7.2 MST Region

An MST region is a logical grouping of multiple network devices that appears as a single device to the rest of the network. Each MSTP-enabled device can only belong to one MST region. When BPDUs enter an MST region, external path cost (of paths outside this region) is increased by one. Internal path cost (of paths within this region) is increased by one when BPDUs traverse the region.

Devices that belong to the same MST region are configured to have the same MSTP configuration identification settings. These include the following parameters:

- Name of the MST region
- Revision level as the unique number for the MST region

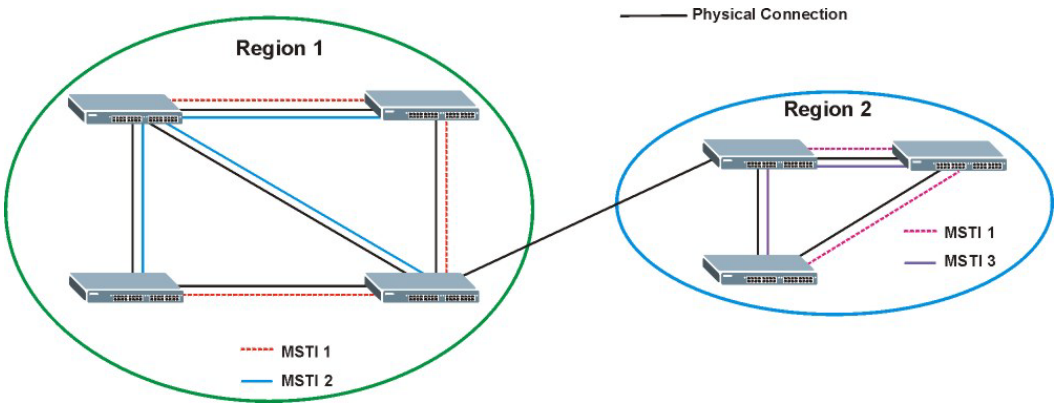
- VLAN-to-MST Instance mapping

13.7.3 MST Instance

An MST Instance (MSTI) is a spanning tree instance. VLANs can be configured to run on a specific MSTI. Each created MSTI is identified by a unique number (known as an MST ID) known internally to a region. Thus an MSTI does not span across MST regions.

The following figure shows an example where there are two MST regions. Regions 1 and 2 have 2 spanning tree instances.

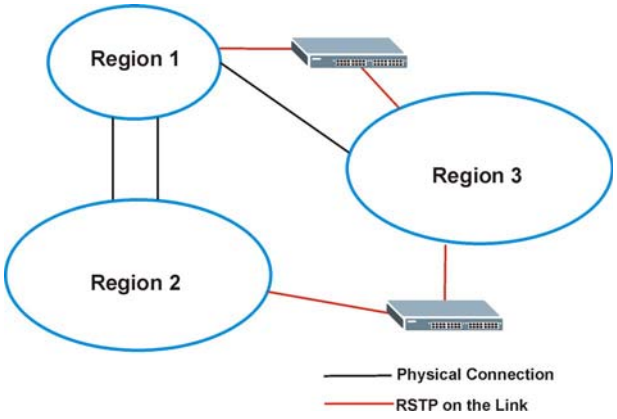
Figure 96 MSTIs in Different Regions



13.7.4 Common and Internal Spanning Tree (CIST)

A CIST represents the connectivity of the entire network and it is equivalent to a spanning tree in an STP/RSTP. The CIST is the default MST instance (MSTID 0). Any VLANs that are not members of an MST instance are members of the CIST. In an MSTP-enabled network, there is only one CIST that runs between MST regions and single spanning tree devices. A network may contain multiple MST regions and other network segments running RSTP.

Figure 97 MSTP and Legacy RSTP Network Example



14

Bandwidth Control

14.1 Overview

This chapter shows you how you can cap the maximum bandwidth using the **Bandwidth Control** screen.

Bandwidth control means defining a maximum allowable bandwidth for incoming and/or out-going traffic flows on a port.

14.1.1 What You Can Do

Use the **Bandwidth Control** screen (Section 14.2 on page 134) to limit the bandwidth for traffic going through the Switch.

14.2 Bandwidth Control Setup

Click **Advanced Application** > **Bandwidth Control** in the navigation panel to bring up the screen as shown next.

Figure 98 Advanced Application > Bandwidth Control

The following table describes the related labels in this screen.

Table 56 Advanced Application > Bandwidth Control

LABEL	DESCRIPTION
Active	Select this check box to enable bandwidth control on the Switch.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to activate ingress rate limits on this port.
Ingress Rate	Specify the maximum bandwidth allowed in kilobits per second (Kbps) for the incoming traffic flow on a port. Note: Ingress rate bandwidth control applies to layer 2 traffic only.
Active	Select this check box to activate egress rate limits on this port.
Egress Rate	Specify the maximum bandwidth allowed in kilobits per second (Kbps) for the out-going traffic flow on a port.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields.

15

Broadcast Storm Control

15.1 Broadcast Storm Control Overview

This chapter introduces and shows you how to configure the broadcast storm control feature.

Broadcast storm control limits the number of broadcast, multicast and destination lookup failure (DLF) packets the Switch receives per second on the ports. When the maximum number of allowable broadcast, multicast and/or DLF packets is reached per second, the subsequent packets are discarded. Enable this feature to reduce broadcast, multicast and/or DLF packets in your network. You can specify limits for each packet type on each port.

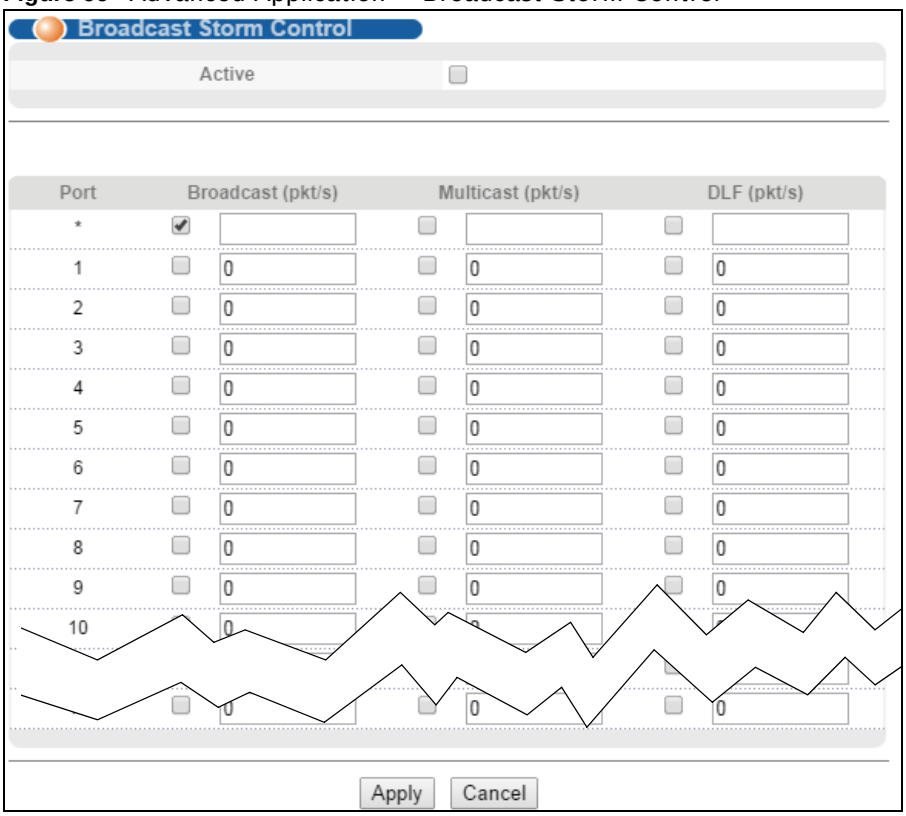
15.1.1 What You Can Do

Use the **Broadcast Storm Control** screen (Section 15.2 on page 136) to limit the number of broadcast, multicast and destination lookup failure (DLF) packets the Switch receives per second on the ports.

15.2 Broadcast Storm Control Setup

Click **Advanced Application** > **Broadcast Storm Control** in the navigation panel to display the screen as shown next.

Figure 99 Advanced Application > Broadcast Storm Control



The following table describes the labels in this screen.

Table 57 Advanced Application > Broadcast Storm Control

LABEL	DESCRIPTION
Active	Select this check box to enable traffic storm control on the Switch. Clear this check box to disable this feature.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Broadcast (pkt/s)	Select this option and specify how many broadcast packets the port receives per second.
Multicast (pkt/s)	Select this option and specify how many multicast packets the port receives per second.
DLF (pkt/s)	Select this option and specify how many destination lookup failure (DLF) packets the port receives per second.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields.

16

Mirroring

16.1 Mirroring Overview

This chapter discusses port mirroring setup screens.

Port mirroring allows you to copy a traffic flow to a monitor port (the port you copy the traffic to) in order that you can examine the traffic from the monitor port without interference.

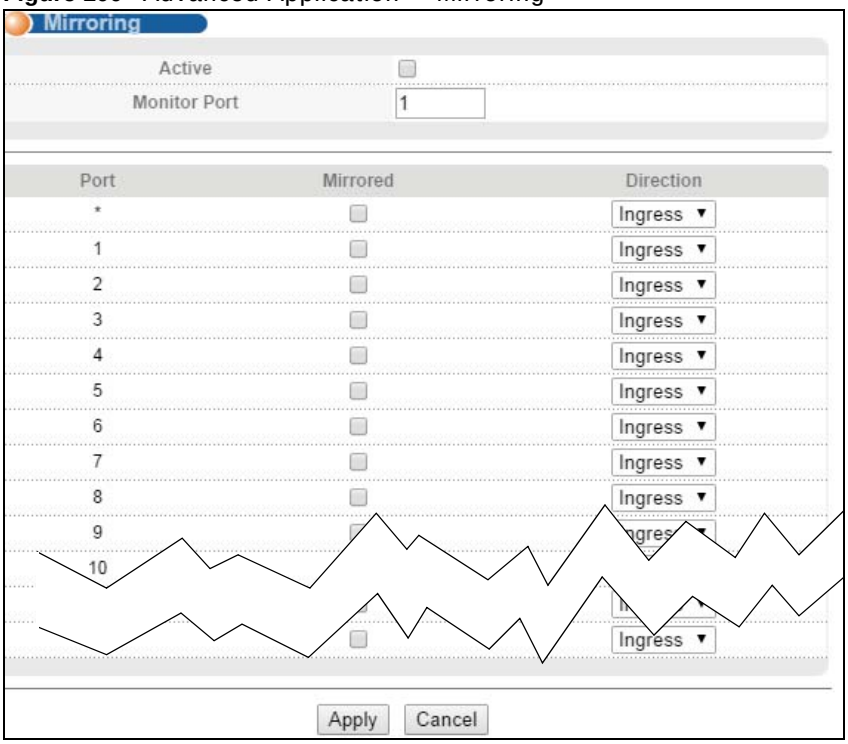
16.1.1 What You Can Do

Use the **Mirroring** screen (Section 16.2 on page 138) to select a monitor port and specify the traffic flow to be copied to the monitor port.

16.2 Port Mirroring Setup

Click **Advanced Application > Mirroring** in the navigation panel to display the **Mirroring** screen. Use this screen to select a monitor port and specify the traffic flow to be copied to the monitor port.

Figure 100 Advanced Application > Mirroring



The following table describes the labels in this screen.

Table 58 Advanced Application > Mirroring

LABEL	DESCRIPTION
Active	Select this check box to activate port mirroring on the Switch. Clear this check box to disable the feature.
Monitor Port	The monitor port is the port you copy the traffic to in order to examine it in more detail without interfering with the traffic flow on the original port(s). Enter the port number of the monitor port.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Mirrored	Select this option to mirror the traffic on a port.
Direction	Specify the direction of the traffic to mirror by selecting from the drop-down list box. Choices are **Egress** (outgoing), **Ingress** (incoming) and **Both**.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields.

17

Link Aggregation

17.1 Overview

This chapter shows you how to logically aggregate physical links to form one logical, higher-bandwidth link.

Link aggregation (trunking) is the grouping of physical ports into one logical higher-capacity link. You may want to trunk ports if for example, it is cheaper to use multiple lower-speed links than to under-utilize a high-speed, but more costly, single-port link. However, the more ports you aggregate then the fewer available ports you have. A trunk group is one logical link containing multiple ports.

The beginning port of each trunk group must be physically connected to form a trunk group.

17.1.1 What You Can Do

- Use the **Link Aggregation Status** screen (Section 17.2 on page 141) to view ports you have configured to be in the trunk group, ports that are currently transmitting data as one logical link in the trunk group and so on.
- Use the **Link Aggregation Setting** screen (Section 17.3 on page 142) to configure to enable static link aggregation.
- Use the **Link Aggregation Control Protocol** screen (Section 17.4 on page 144) to enable Link Aggregation Control Protocol (LACP).

17.1.2 What You Need to Know

The Switch supports both static and dynamic link aggregation.

Note: In a properly planned network, it is recommended to implement static link aggregation only. This ensures increased network stability and control over the trunk groups on your Switch.

See Section 17.5.1 on page 146 for a static port trunking example.

Dynamic Link Aggregation

The Switch adheres to the IEEE 802.3ad standard for static and dynamic (LACP) port trunking.

The IEEE 802.3ad standard describes the Link Aggregation Control Protocol (LACP) for dynamically creating and managing trunk groups.

When you enable LACP link aggregation on a port, the port can automatically negotiate with the ports at the remote end of a link to establish trunk groups. LACP also allows port redundancy, that

is, if an operational port fails, then one of the “standby” ports become operational without user intervention. Please note that:

- You must connect all ports point-to-point to the same Ethernet switch and configure the ports for LACP trunking.
- LACP only works on full-duplex links.
- All ports in the same trunk group must have the same media type, speed, duplex mode and flow control settings.

Configure trunk groups or LACP before you connect the Ethernet switch to avoid causing network topology loops.

Link Aggregation ID

LACP aggregation ID consists of the following information:

Table 59 Link Aggregation ID: Local Switch

SYSTEM PRIORITY	MAC ADDRESS	KEY	PORT PRIORITY	PORT NUMBER
0000	00-00-00-00-00-00	0000	00	0000

Table 60 Link Aggregation ID: Peer Switch

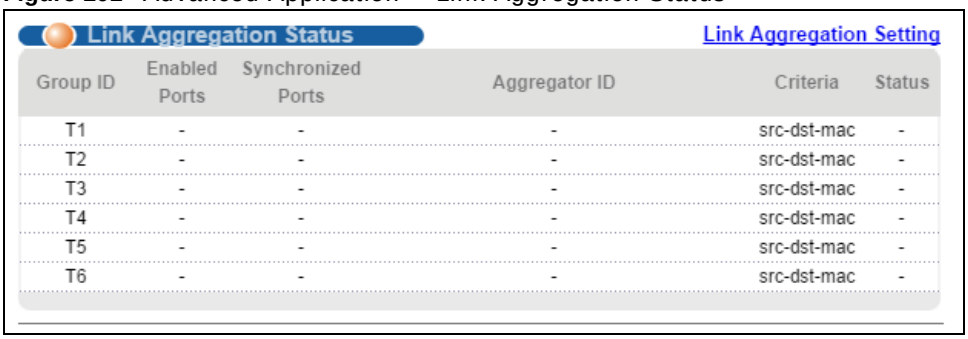
SYSTEM PRIORITY	MAC ADDRESS	KEY	PORT PRIORITY	PORT NUMBER
0000	00-00-00-00-00-00	0000	00	0000

Port Priority and Port Number are 0 as it is the aggregator ID for the trunk group, not the individual port.

17.2 Link Aggregation Status

Click **Advanced Application** > **Link Aggregation** in the navigation panel. The **Link Aggregation Status** screen displays by default. See Section 17.1 on page 140 for more information.

Figure 101 Advanced Application > Link Aggregation Status



The following table describes the labels in this screen.

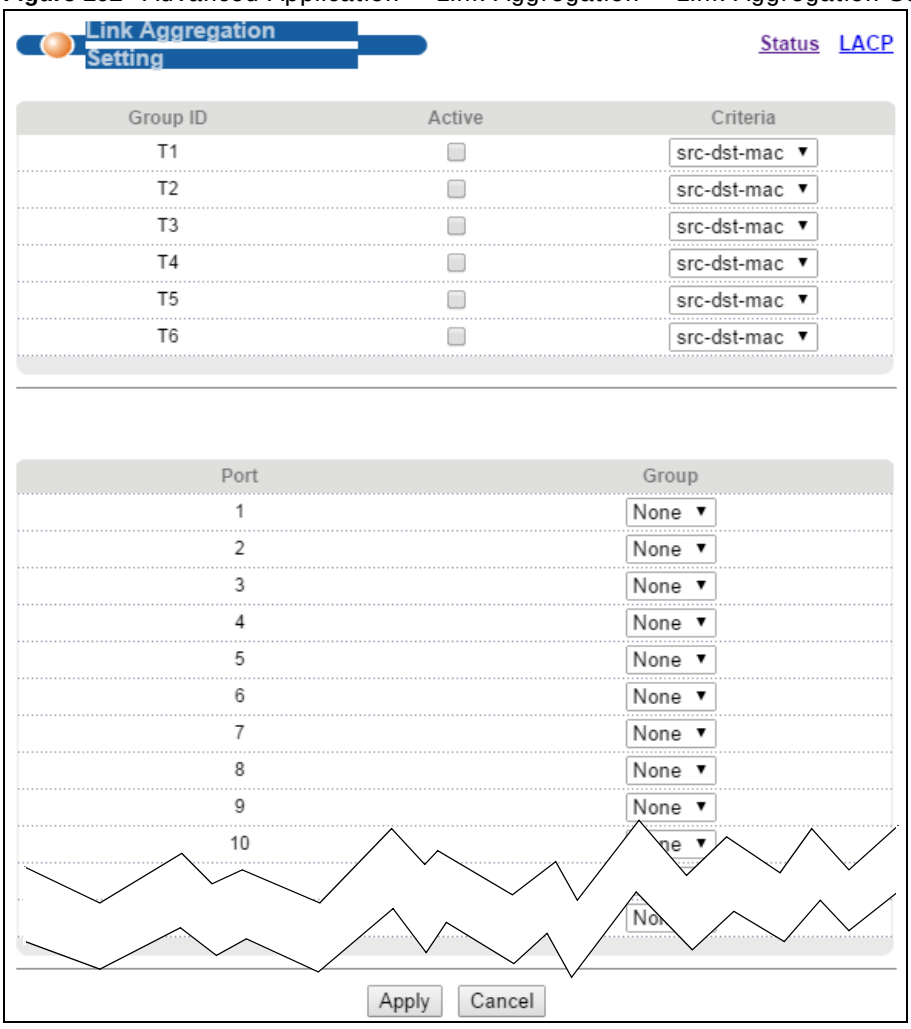
Table 61 Advanced Application > Link Aggregation Status

LABEL	DESCRIPTION
Group ID	This field displays the group ID to identify a trunk group, that is, one logical link containing multiple ports.
Enabled Ports	These are the ports you have configured in the **Link Aggregation** screen to be in the trunk group. The port number(s) displays only when this trunk group is activated and there is a port belonging to this group.
Synchronized Ports	These are the ports that are currently transmitting data as one logical link in this trunk group.
Aggregator ID	Link Aggregator ID consists of the following: system priority, MAC address, key, port priority and port number. Refer to Section on page 141 for more information on this field. The ID displays only when there is a port belonging to this trunk group and LACP is also enabled for this group.
Criteria	This shows the outgoing traffic distribution algorithm used in this trunk group. Packets from the same source and/or to the same destination are sent over the same link within the trunk. **src-mac** means the Switch distributes traffic based on the packet's source MAC address. **dst-mac** means the Switch distributes traffic based on the packet's destination MAC address. **src-dst-mac** means the Switch distributes traffic based on a combination of the packet's source and destination MAC addresses. **src-ip** means the Switch distributes traffic based on the packet's source IP address. **dst-ip** means the Switch distributes traffic based on the packet's destination IP address. **src-dst-ip** means the Switch distributes traffic based on a combination of the packet's source and destination IP addresses.
Status	This field displays how these ports were added to the trunk group. It displays: • **Static** - if the ports are configured as static members of a trunk group. • **LACP** - if the ports are configured to join a trunk group via LACP.

17.3 Link Aggregation Setting

Click **Advanced Application** > **Link Aggregation > Link Aggregation Setting** to display the screen shown next. See Section 17.1 on page 140 for more information on link aggregation.

Figure 102 Advanced Application > Link Aggregation > Link Aggregation Setting



The following table describes the labels in this screen.

Table 62 Advanced Application > Link Aggregation > Link Aggregation Setting

LABEL	DESCRIPTION
Link Aggregation Setting	This is the only screen you need to configure to enable static link aggregation.
Group ID	The field identifies the link aggregation group, that is, one logical link containing multiple ports.
Active	Select this option to activate a trunk group.

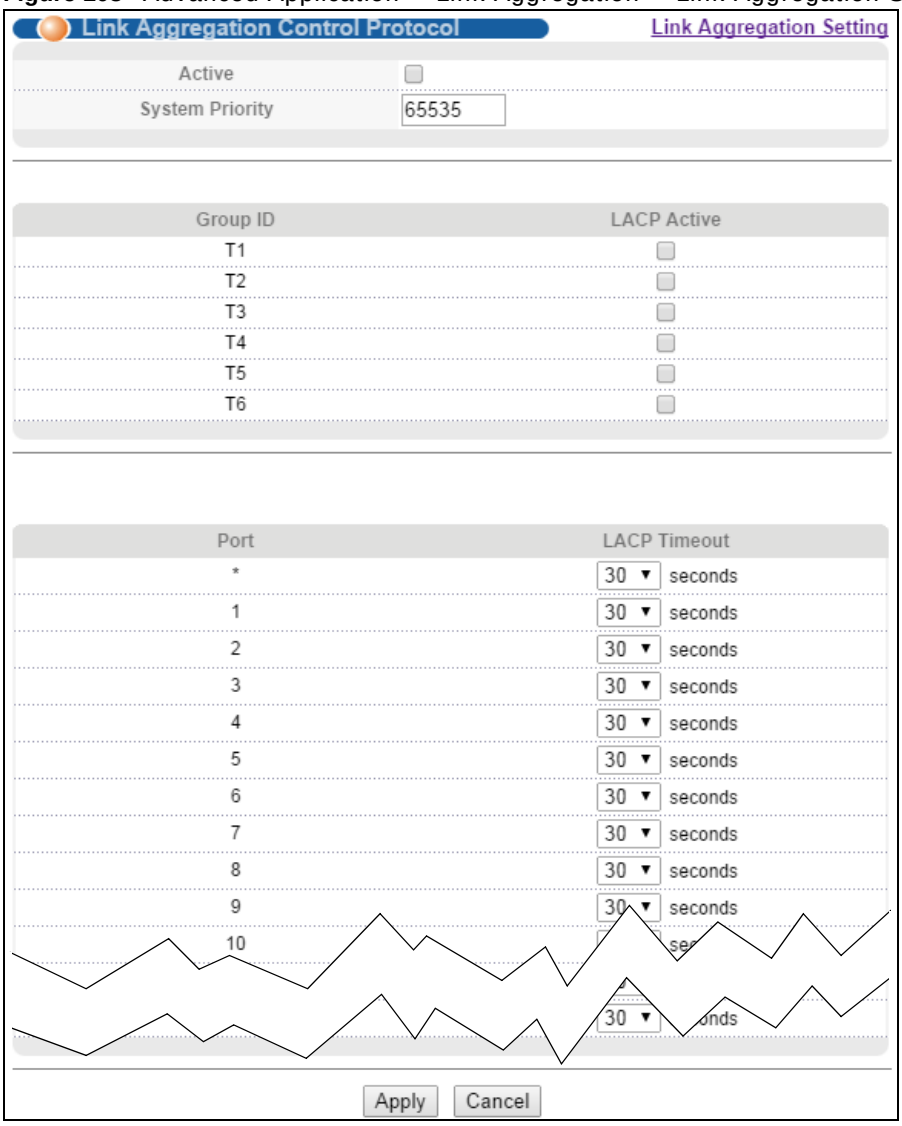
Table 62 Advanced Application > Link Aggregation > Link Aggregation Setting (continued)

LABEL	DESCRIPTION
Criteria	Select the outgoing traffic distribution type. Packets from the same source and/or to the same destination are sent over the same link within the trunk. By default, the Switch uses the **src-dst-mac** distribution type. If the Switch is behind a router, the packet's destination or source MAC address will be changed. In this case, set the Switch to distribute traffic based on its IP address to make sure port trunking can work properly. Select **src-mac** to distribute traffic based on the packet's source MAC address. Select **dst-mac** to distribute traffic based on the packet's destination MAC address. Select **src-dst-mac** to distribute traffic based on a combination of the packet's source and destination MAC addresses. Select **src-ip** to distribute traffic based on the packet's source IP address. Select **dst-ip** to distribute traffic based on the packet's destination IP address. Select **src-dst-ip** to distribute traffic based on a combination of the packet's source and destination IP addresses.
Port	This field displays the port number.
Group	Select the trunk group to which a port belongs. Note: When you enable the port security feature on the Switch and configure port security settings for a port, you cannot include the port in an active trunk group.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

17.4 Link Aggregation Control Protocol

Click **Advanced Application** > **Link Aggregation** > **Link Aggregation Setting** > **LACP** to display the screen shown next. See Section on page 140 for more information on dynamic link aggregation.

Figure 103 Advanced Application > Link Aggregation > Link Aggregation Setting > LACP



The following table describes the labels in this screen.

Table 63 Advanced Application > Link Aggregation > Link Aggregation Setting > LACP

LABEL	DESCRIPTION
Link Aggregation Control Protocol	Note: Do not configure this screen unless you want to enable dynamic link aggregation.
Active	Select this checkbox to enable Link Aggregation Control Protocol (LACP).
System Priority	LACP system priority is a number between 1 and 65,535. The switch with the lowest system priority (and lowest port number if system priority is the same) becomes the LACP "server". The LACP "server" controls the operation of LACP setup. Enter a number to set the priority of an active port using Link Aggregation Control Protocol (LACP). The smaller the number, the higher the priority level.
Group ID	The field identifies the link aggregation group, that is, one logical link containing multiple ports.
LACP Active	Select this option to enable LACP for a trunk.

Table 63 Advanced Application > Link Aggregation > Link Aggregation Setting > LACP (continued)

LABEL	DESCRIPTION
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
LACP Timeout	Timeout is the time interval between the individual port exchanges of LACP packets in order to check that the peer port in the trunk group is still up. If a port does not respond after three tries, then it is deemed to be “down” and is removed from the trunk. Set a short timeout (one second) for busy trunked links to ensure that disabled ports are removed from the trunk group as soon as possible. Select either 1 second or 30 seconds.
Apply	Click **Apply** to save your changes to the Switch’s run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

17.5 Technical Reference

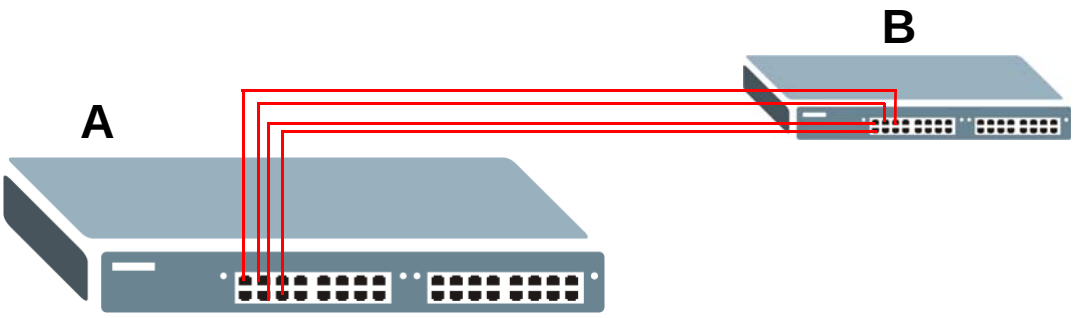
This section provides technical background information on the topics discussed in this chapter.

17.5.1 Static Trunking Example

This example shows you how to create a static port trunk group for ports 2-5.

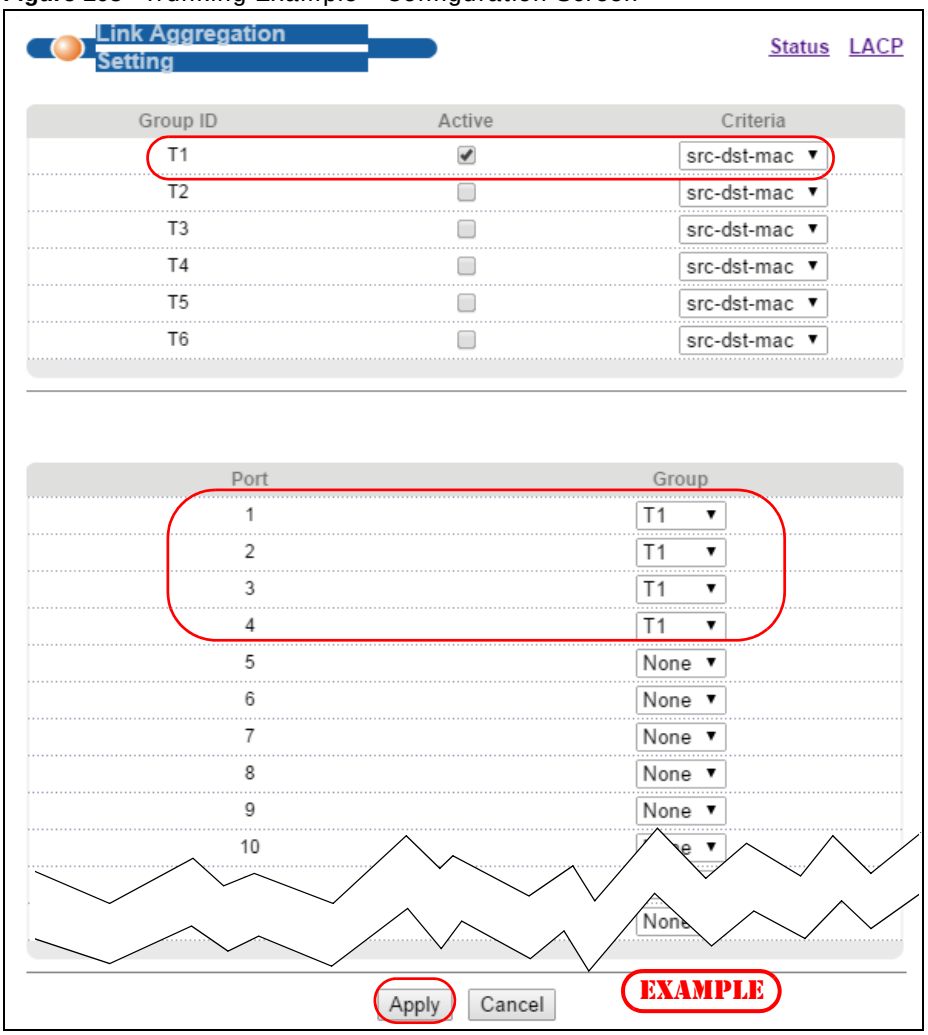
1 **Make your physical connections** - make sure that the ports that you want to belong to the trunk group are connected to the same destination. The following figure shows ports 2-5 on switch **A** connected to switch **B**.

Figure 104 Trunking Example - Physical Connections



2 **Configure static trunking** - Click **Advanced Application** > **Link Aggregation** > **Link Aggregation Setting**. In this screen activate trunk group **T1**, select the traffic distribution algorithm used by this group and select the ports that should belong to this group as shown in the figure below. Click **Apply** when you are done.

Figure 105 Trunking Example - Configuration Screen



Your trunk group 1 (**T1**) configuration is now complete.

18

Port Authentication

18.1 Port Authentication Overview

This chapter describes the IEEE 802.1x authentication method. Port authentication is a way to validate access to ports on the Switch to clients based on an external server (authentication server). The Switch supports the following methods for port authentication:

- **IEEE 802.1x**[1] - An authentication server validates access to a port based on a username and password provided by the user.
- **MAC** - An authentication server validates access to a port based on the MAC address and password of the client.

Both types of authentication use the RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) protocol to validate users.

If you enable IEEE 802.1x authentication and MAC authentication on the same port, the Switch performs IEEE 802.1x authentication first. If a user fails to authenticate via the IEEE 802.1x method, then access to the port is denied.

18.1.1 What You Need to Know

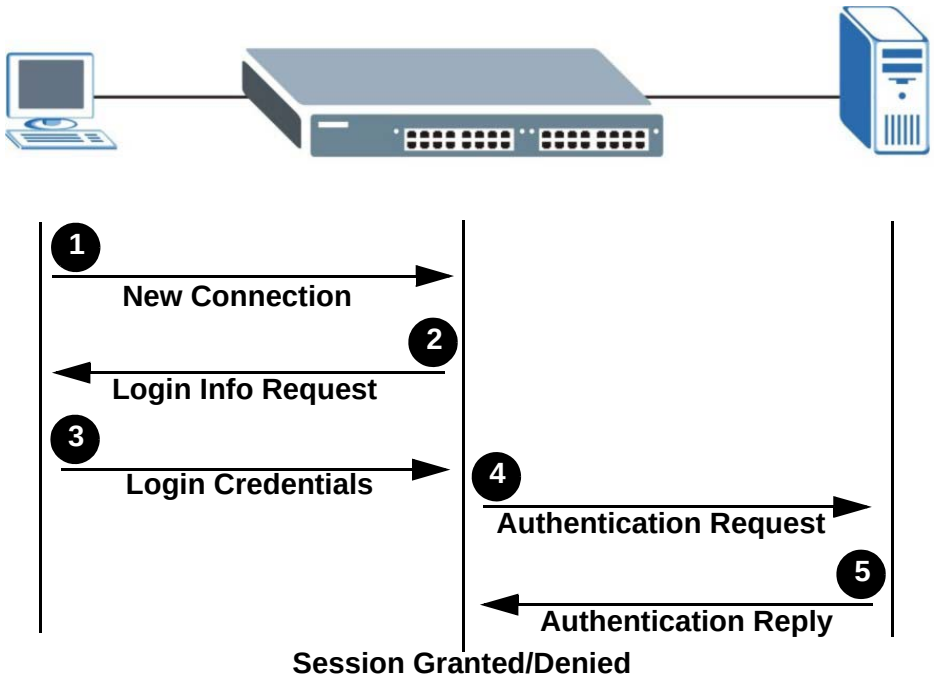
IEEE 802.1x authentication uses the RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) protocol to validate users. See RADIUS and TACACS+ for more information on configuring your RADIUS server settings.

IEEE 802.1x Authentication

The following figure illustrates how a client connecting to a IEEE 802.1x authentication enabled port goes through a validation process. The Switch prompts the client for login information in the form of a user name and password. When the client provides the login credentials, the Switch sends an authentication request to a RADIUS server. The RADIUS server validates whether this client is allowed access to the port.

1. At the time of writing, IEEE 802.1x is not supported by all operating systems. See your operating system documentation. If your operating system does not support 802.1x, then you may need to install 802.1x client software.

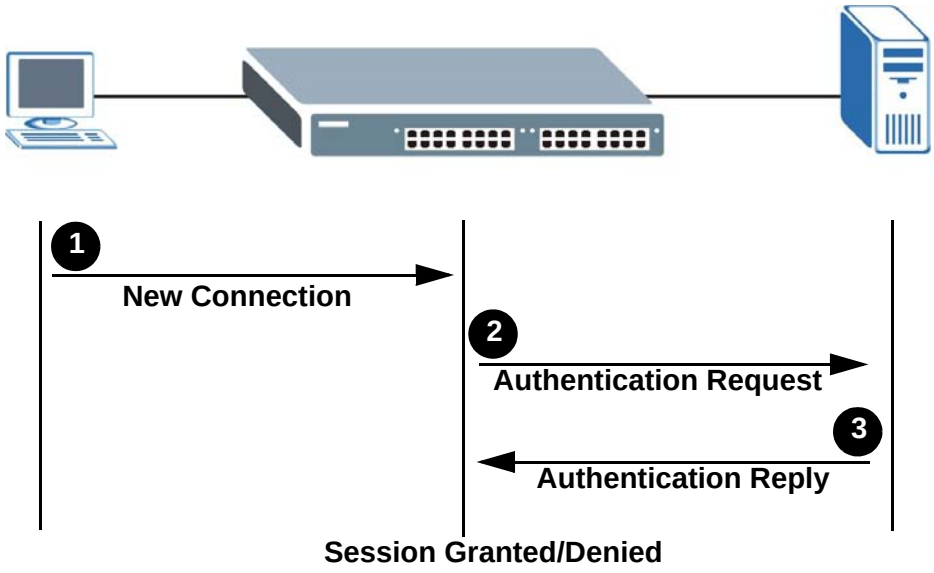
Figure 106 IEEE 802.1x Authentication Process



18.1.2 MAC Authentication

MAC authentication works in a very similar way to IEEE 802.1x authentication. The main difference is that the Switch does not prompt the client for login credentials. The login credentials are based on the source MAC address of the client connecting to a port on the Switch along with a password configured specifically for MAC authentication on the Switch.

Figure 107 MAC Authentication Process

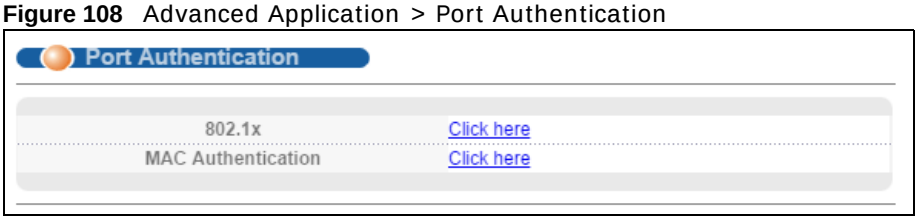


18.2 Port Authentication Configuration

To enable port authentication, first activate the port authentication method (both on the Switch and the port(s)) then configure the RADIUS server settings in the **Auth and Acct > Radius Server Setup** screen.

Click **Advanced Application** > **Port Authentication** in the navigation panel to display the screen as shown.

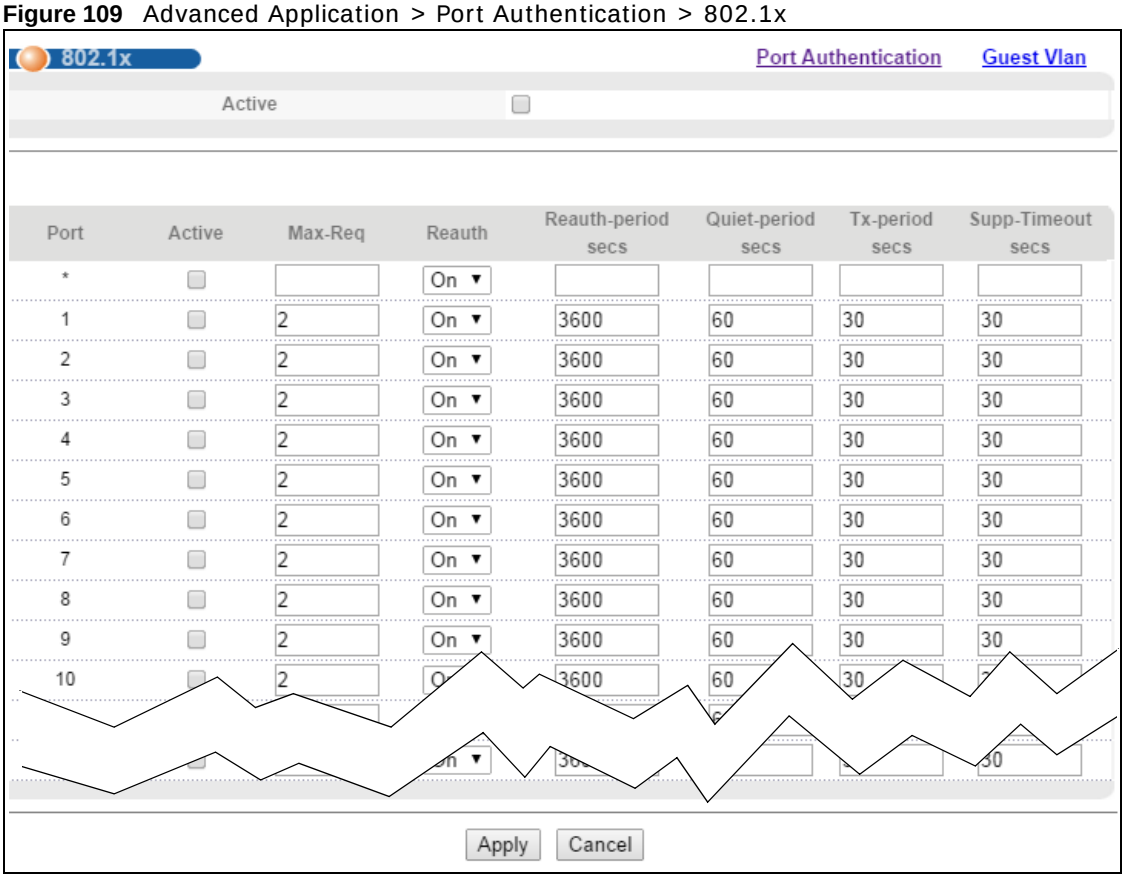
Figure 108 Advanced Application > Port Authentication



18.3 Activate IEEE 802.1x Security

Use this screen to activate IEEE 802.1x security. In the **Port Authentication** screen click **802.1x** to display the configuration screen as shown.

Figure 109 Advanced Application > Port Authentication > 802.1x



The following table describes the labels in this screen.

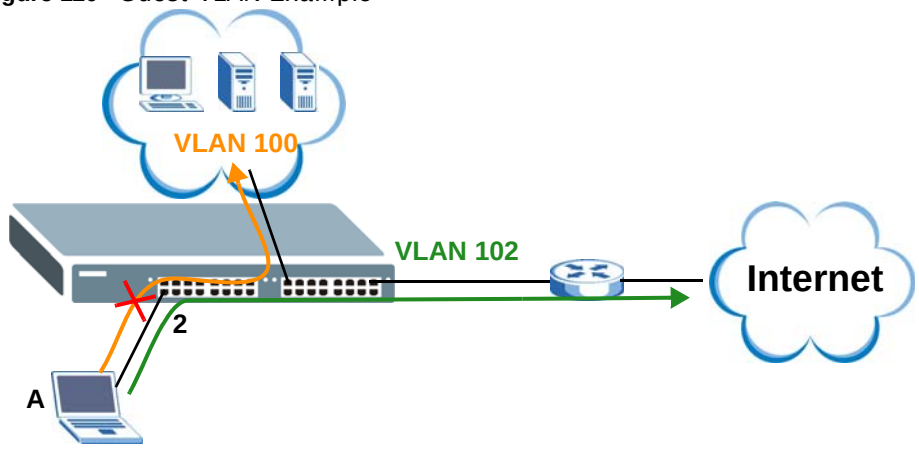
Table 64 Advanced Application > Port Authentication > 802.1x

LABEL	DESCRIPTION
Active	Select this check box to permit 802.1x authentication on the Switch. Note: You must first enable 802.1x authentication on the Switch before configuring it on each port.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this to permit 802.1x authentication on this port. You must first allow 802.1x authentication on the Switch before configuring it on each port.
Max-Req	Specify the number of times the Switch tries to authenticate client(s) before sending unresponsive ports to the Guest VLAN. This is set to 2 by default. That is, the Switch attempts to authenticate a client twice. If the client does not respond to the first authentication request, the Switch tries again. If the client still does not respond to the second request, the Switch sends the client to the Guest VLAN. The client needs to send a new request to be authenticated by the Switch again.
Reauth	Specify if a subscriber has to periodically re-enter his or her username and password to stay connected to the port.
Reauth-period secs	Specify the length of time required to pass before a client has to re-enter his or her username and password to stay connected to the port.
Quiet-period secs	Specify the number of seconds the port remains in the HELD state and rejects further authentication requests from the connected client after a failed authentication exchange.
Tx-period secs	Specify the number of seconds the Switch waits for client's response before re-sending an identity request to the client.
Supp-Timeout secs	Specify the number of seconds the Switch waits for client's response to a challenge request before sending another request.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

18.3.1 Guest VLAN

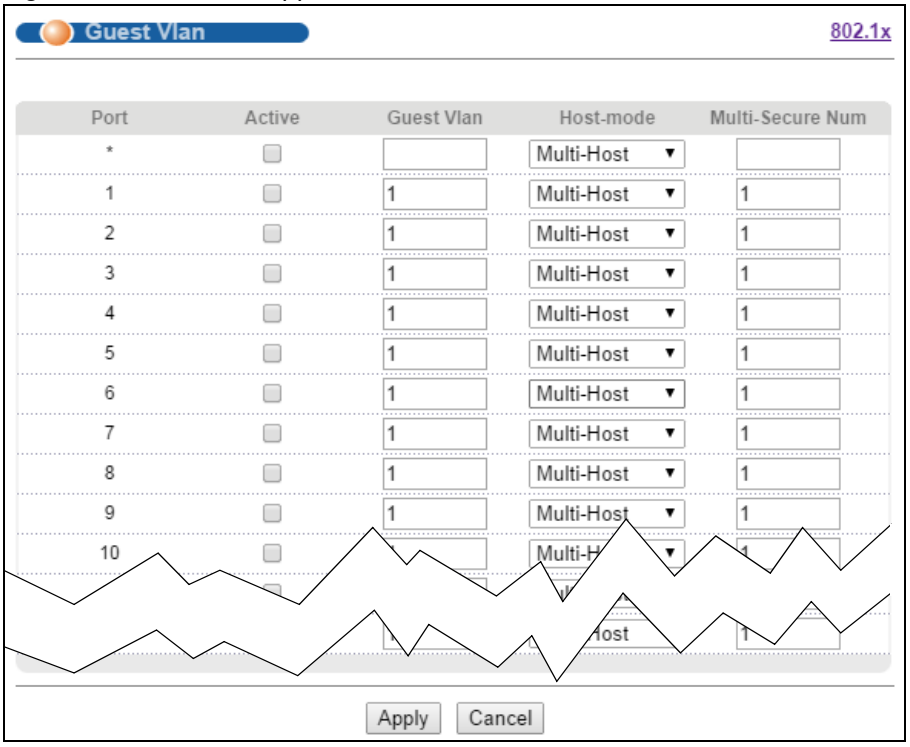
When 802.1x port authentication is enabled on the Switch and its ports, clients that do not have the correct credentials are blocked from using the port(s). You can configure your Switch to have one VLAN that acts as a guest VLAN. If you enable the guest VLAN (**102** in the example) on a port (**2** in the example), the user (**A** in the example) that is not IEEE 802.1x capable or fails to enter the correct username and password can still access the port, but traffic from the user is forwarded to the guest VLAN. That is, unauthenticated users can have access to limited network resources in the same guest VLAN, such as the Internet. The rights granted to the Guest VLAN depends on how the network administrator configures switches or routers with the guest network feature.

Figure 110 Guest VLAN Example



Use this screen to enable and assign a guest VLAN to a port. In the **Port Authentication > 802.1x** screen click **Guest Vlan** to display the configuration screen as shown.

Figure 111 Advanced Application > Port Authentication > 802.1x > Guest VLAN



The following table describes the labels in this screen.

Table 65 Advanced Application > Port Authentication > 802.1x > Guest VLAN

LABEL	DESCRIPTION
Port	This field displays a port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Changes in this row are copied to all the ports as soon as you make them.

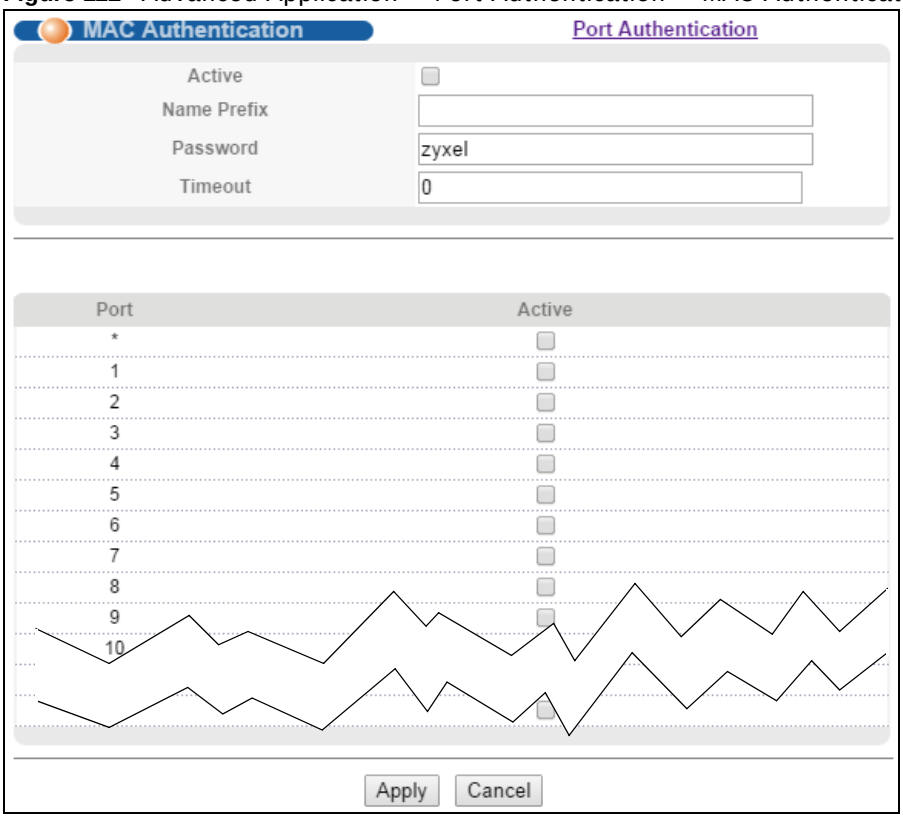
Table 65 Advanced Application > Port Authentication > 802.1x > Guest VLAN (continued)

LABEL	DESCRIPTION
Active	Select this checkbox to enable the guest VLAN feature on this port. Clients that fail authentication are placed in the guest VLAN and can receive limited services.
Guest Vlan	A guest VLAN is a pre-configured VLAN on the Switch that allows non-authenticated users to access limited network resources through the Switch. You must also enable IEEE 802.1x authentication on the Switch and the associated ports. Enter the number that identifies the guest VLAN. Make sure this is a VLAN recognized in your network.
Host-mode	Specify how the Switch authenticates users when more than one user connect to the port (using a hub). Select **Multi-Host** to authenticate only the first user that connects to this port. If the first user enters the correct credential, any other users are allowed to access the port without authentication. If the first user fails to enter the correct credential, they are all put in the guest VLAN. Once the first user who did authentication logs out or disconnects from the port, rest of the users are blocked until a user does the authentication process again. Select **Multi-Secure** to authenticate each user that connects to this port.
Multi-Secure Num	If you set **Host-mode** to **Multi-Secure**, specify the maximum number of users that the Switch will authenticate on this port.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

18.3.2 Activate MAC Authentication

Use this screen to activate MAC authentication. In the **Port Authentication** screen click **MAC Authentication** to display the configuration screen as shown.

Figure 112 Advanced Application > Port Authentication > MAC Authentication



The following table describes the labels in this screen.

Table 66 Advanced Application > Port Authentication > MAC Authentication

LABEL	DESCRIPTION
Active	Select this check box to permit MAC authentication on the Switch. Note: You must first enable MAC authentication on the Switch before configuring it on each port.
Name Prefix	Type the prefix that is appended to all MAC addresses sent to the RADIUS server for authentication. You can enter up to 32 printable ASCII characters. If you leave this field blank, then only the MAC address of the client is forwarded to the RADIUS server.
Password	Type the password the Switch sends along with the MAC address of a client for authentication with the RADIUS server. You can enter up to 32 printable ASCII characters.
Timeout	Specify the amount of time before the Switch allows a client MAC address that fails authentication to try and authenticate again. Maximum time is 3000 seconds. When a client fails MAC authentication, its MAC address is learned by the MAC address table with a status of denied. The timeout period you specify here is the time the MAC address entry stays in the MAC address table until it is cleared. If you specify 0 for the timeout value, then this entry will not be deleted from the MAC address table. Note: If the **Aging Time** in the **Switch Setup** screen is set to a lower value, then it supersedes this setting. See Section 8.5 on page 63.
Port	This field displays a port number.

Table 66 Advanced Application > Port Authentication > MAC Authentication (continued)

LABEL	DESCRIPTION
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to permit MAC authentication on this port. You must first allow MAC authentication on the Switch before configuring it on each port.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

19

Port Security

19.1 Port Security Overview

This chapter shows you how to set up port security.

Port security allows only packets with dynamically learned MAC addresses and/or configured static MAC addresses to pass through a port on the Switch. The Switch can learn up to 16K MAC addresses in total with no limit on individual ports other than the sum cannot exceed 16K.

For maximum port security, enable this feature, disable MAC address learning and configure static MAC address(es) for a port. It is not recommended you disable port security together with MAC address learning as this will result in many broadcasts. By default, MAC address learning is still enabled even though the port security is not activated.

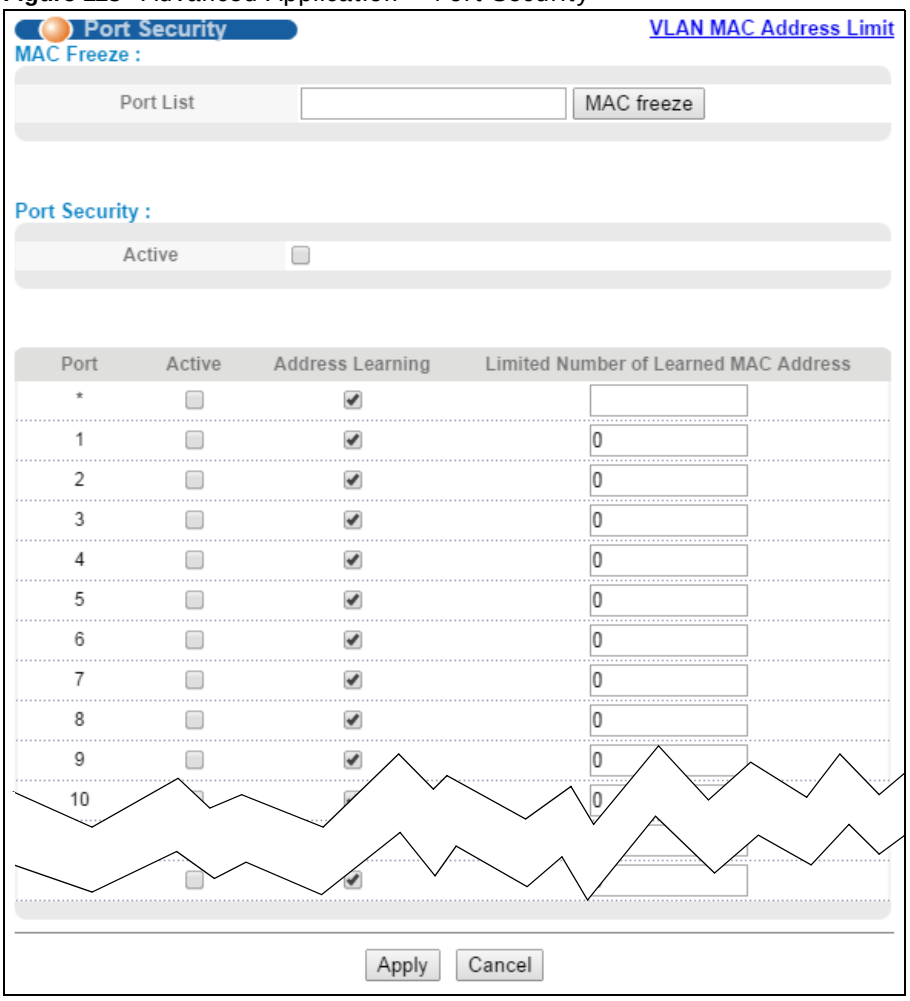
19.1.1 What You Can Do

Use the **Port Security** screen (Section 19.2 on page 156) to enable port security and disable MAC address learning. You can also enable the port security feature on a port.

19.2 Port Security Setup

Click **Advanced Application > Port Security** in the navigation panel to display the screen as shown.

Figure 113 Advanced Application > Port Security



The following table describes the labels in this screen.

Table 67 Advanced Application > Port Security

LABEL	DESCRIPTION
Port List	Enter the number of the port(s) (separated by a comma) on which you want to enable port security and disable MAC address learning. After you click **MAC freeze**, all previously learned MAC addresses on the specified port(s) will become static MAC addresses and display in the **Static MAC Forwarding** screen.
MAC freeze	Click **MAC freeze** to have the Switch automatically select the **Active** check boxes and clear the **Address Learning** check boxes only for the ports specified in the **Port list**.
Active	Select this option to enable port security on the Switch.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.

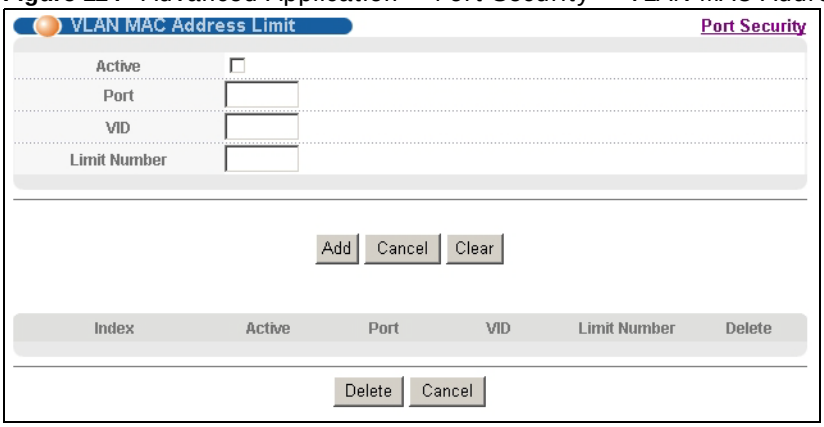
Table 67 Advanced Application > Port Security (continued)

LABEL	DESCRIPTION
Active	Select this check box to enable the port security feature on this port. The Switch forwards packets whose MAC address(es) is in the MAC address table on this port. Packets with no matching MAC address(es) are dropped. Clear this check box to disable the port security feature. The Switch forwards all packets on this port.
Address Learning	MAC address learning reduces outgoing broadcast traffic. For MAC address learning to occur on a port, the port itself must be active with address learning enabled.
Limited Number of Learned MAC Address	Use this field to limit the number of (dynamic) MAC addresses that may be learned on a port. For example, if you set this field to "5" on port 2, then only the devices with these five learned MAC addresses may access port 2 at any one time. A sixth device would have to wait until one of the five learned MAC addresses aged out. MAC address aging out time can be set in the **Switch Setup** screen. The valid range is from "0" to "16384". "0" means this feature is disabled.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

19.3 VLAN MAC Address Limit

Use this screen to set the MAC address learning limit on per-port and per-VLAN basis. Click **VLAN MAC Address Limit** in the **Advanced Application > Port Security** screen to display the screen as shown.

Figure 114 Advanced Application > Port Security > VLAN MAC Address Limit



The following table describes the labels in this screen.

Table 68 Advanced Application > Port Security > VLAN MAC Address Limit

LABEL	DESCRIPTION
Active	Select this option to activate this rule.
Port	Enter the number of the port to which this rule is applied.
VID	Enter the VLAN identification number.

Table 68 Advanced Application > Port Security > VLAN MAC Address Limit (continued)

LABEL	DESCRIPTION
Limit Number	Use this field to limit the number of (dynamic) MAC addresses that may be learned on a port in a specified VLAN. For example, if you set this field to "5" on port 2, then only the devices with these five learned MAC addresses may access port 2 at any one time. A sixth device would have to wait until one of the five learned MAC addresses aged out. MAC address aging out time can be set in the **Switch Setup** screen. The valid range is from "0" to "16K". "0" means this feature is disabled.
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to your previous configuration.
Clear	Click **Clear** to reset the fields to the factory defaults.
Index	This field displays the index number of the rule. Click an index number to change the settings.
Active	This field displays **Yes** when the rule is activated and **No** when is it deactivated.
Port	This field displays the number of the port to which this rule is applied.
VID	This is the VLAN ID number to which the port belongs.
Limit Number	This is the maximum number of MAC addresses which a port can learn in a VLAN.
Delete	Check the rule(s) that you want to remove in the **Delete** column and then click the **Delete** button.
Cancel	Click **Cancel** to clear the selected checkbox(es) in the **Delete** column.

20

Time Range

This chapter shows you how to set up a time range for time-oriented features on the Switch.

20.1 About Time Range

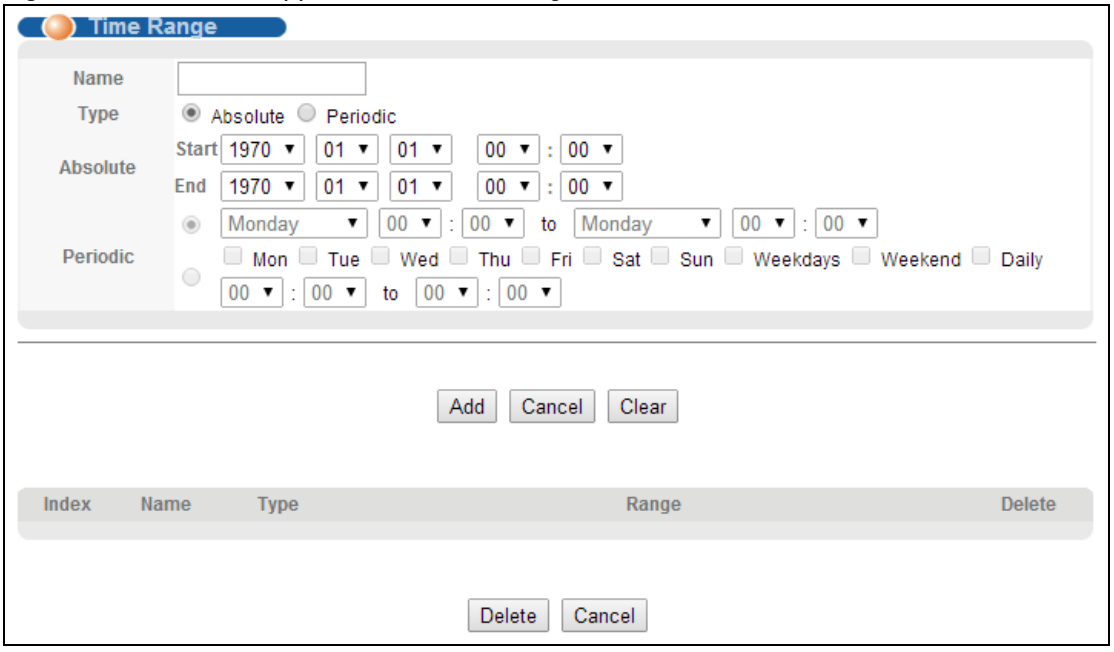
You can set a time range for time-oriented features such as Classifier ACL (Access Control List) rule which categorizes data packets into different network traffic flow. The advantage of the time range feature is that it allows you to schedule the active time of configurations. For example, see Section 21.2 on page 162 to configure the classifier rule with time range.

The time range can be configured in two ways - Absolute and Periodic. Absolute is a fixed time range with a start and end time. Periodic is recurrence of a time range and doesn't have an end time.

20.2 Time Range Setup

Click **Advanced Application** > **Time Range** in the navigation panel to display the screen as shown.

Figure 115 Advanced Application > Time Range



The following table describes the labels in this screen.

Table 69 Advanced Application > Time Range

LABEL	DESCRIPTION
Name	Type a name for this time range rule.
Type	Select a time range type. **Absolute** is a fixed time range that has a set start and end date. **Periodic** is recurrence of a time range.
Absolute	This sets a fixed time range.
Start/End Days of the week	Use the drop-down list box to select a start date, time, an end date, time and days of the week for this time range rule.
Periodic	This sets a recurrent time range.
Days of the week Time	Use the check boxes and drop-down list boxes to set the periodic time range. This is a recurrence time range.
Add	Click **Add** to save the time range you entered.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to reset the fields to the factory defaults.
Index	This field displays the index number of the rule. Click an index number to change the settings.
Name	This field displays the name of the time range rule.
Type	This field displays whether the time range rule is absolute or periodic.
Range	This field displays the time range you entered for this rule.
Delete	You can delete this time range by clicking the check box of this time range rule and click Delete button below.
Delete	Check the rule(s) that you want to remove in the **Delete** column and then click the **Delete** button.
Cancel	Click **Cancel** to clear the selected checkbox(es) in the **Delete** column.

21

Classifier

21.1 Overview

This chapter introduces and shows you how to configure the packet classifier on the Switch. It also discusses Quality of Service (QoS) and classifier concepts as employed by the Switch.

21.1.1 What You Can Do

Use the **Classifier Status** screen (Section 21.2 on page 162) to define the classifiers and view a summary of the classifier configuration. After you define the classifier, you can specify actions (or policy) to act upon the traffic that matches the rules.

21.1.2 What You Need to Know

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical application such as video-on-demand.

A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming port number. For example, you can configure a classifier to select traffic from the same protocol port to form a flow.

Configure QoS on the Switch to group and prioritize application traffic and fine-tune network performance. Setting up QoS involves two separate steps:

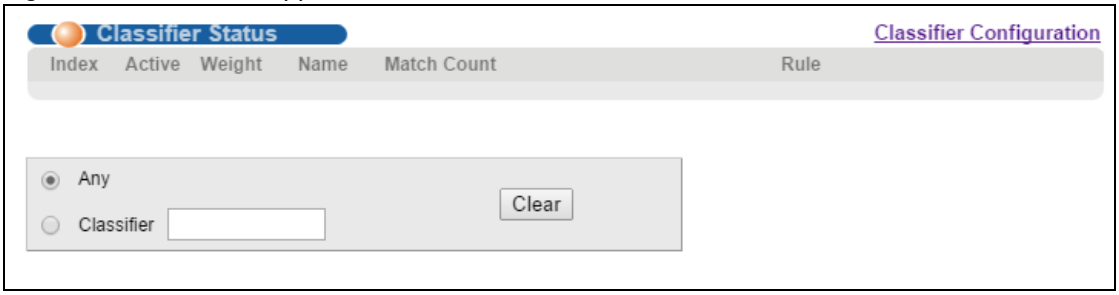
1. Configure classifiers to sort traffic into different flows.
2. Configure policy rules to define actions to be performed on a classified traffic flow (refer to Chapter 22 on page 171 to configure policy rules).

21.2 Classifier Status

Use the **Classifier Configuration** screen to define the classifiers. After you define the classifier, you can specify actions (or policy) to act upon the traffic that matches the rules. Use the **Classifier Status** screen to view a summary of the classifiers configured. To configure policy rules, refer to Chapter 22 on page 171.

Click **Advanced Application** > **Classifier** in the navigation panel to display the configuration Status screen as shown.

Figure 116 Advanced Application > Classifier Status



The following table describes the labels in this screen.

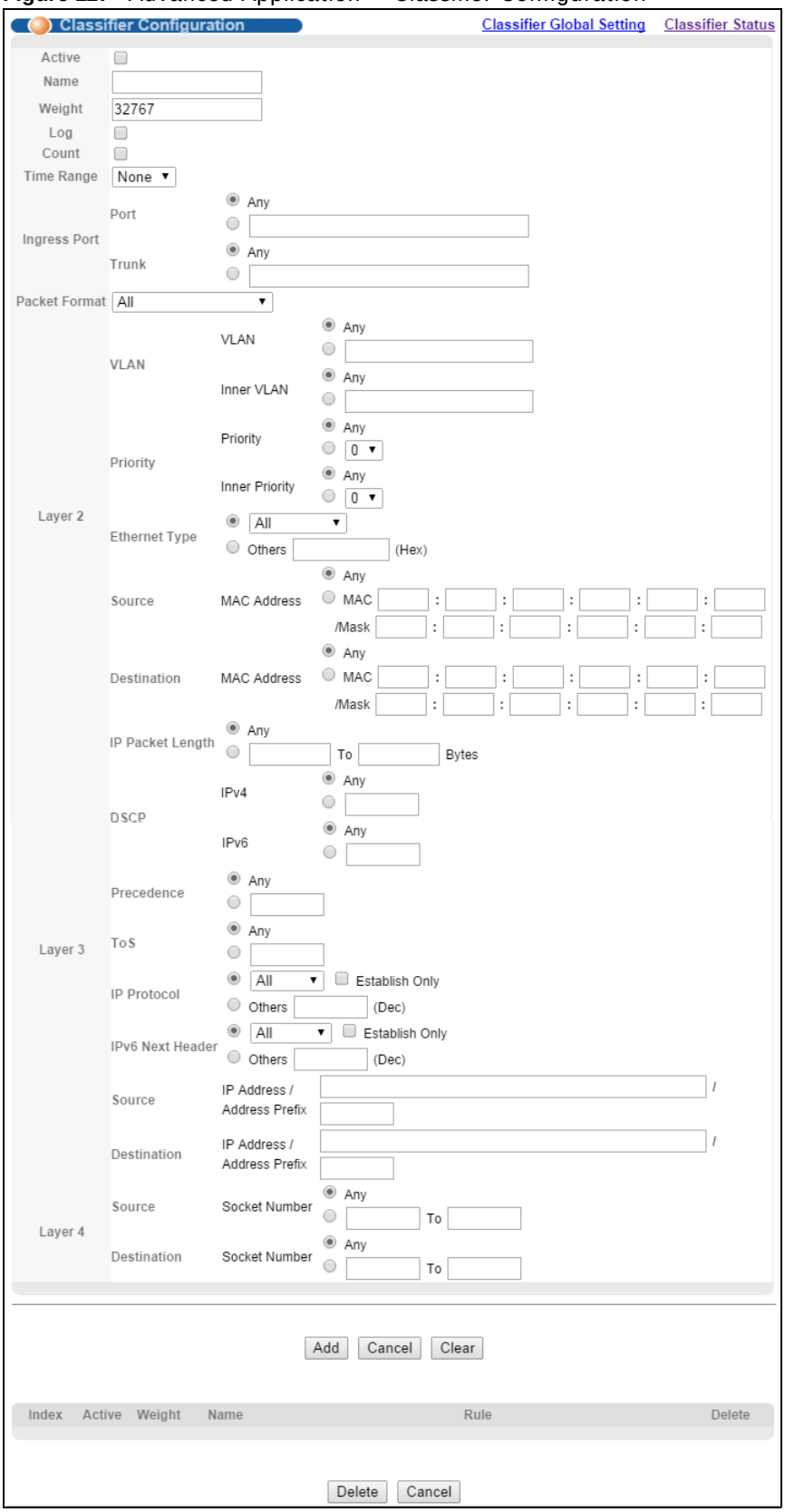
Table 70 Advanced Application > Classifier Status

LABEL	DESCRIPTION
Index	This field displays the index number of the Classifier rule.
Active	This field displays **Yes** when the rule is activated and **No** when it is deactivated.
Weight	This field displays the weight the priority of the Classifier rule when the match order is in **manual** mode. A higher weight means a higher priority.
Match Count	This field displays the number of packets that matched this rule. It displays '-' if the rule does not have count enabled.
Rule	This field displays the name of the Access Control List rule.
Any	Select **Any**, then click **Clear** to clear the matched count for all classifiers.
Classifier	Select **Classifier**, type a classifier name in the text box, then click **Clear** to clear the matched count for that classifier.

21.3 Classifier Configuration

Click **Classifier Configuration** in the **Classifier Status** screen to display the configuration screen as shown.

Figure 117 Advanced Application > Classifier Configuration



The following table describes the labels in this screen.

Table 71 Advanced Application > Classifier > Classifier Configuration

LABEL	DESCRIPTION
Active	Select this option to enable this rule.
Name	Enter a descriptive name for this rule for identifying purposes.
Weight	Enter a number from 0-65535 for the order priority of the Classifier rule. When the match order is in **manual** mode, a higher weight means a higher priority. When the match order is in **auto** mode, the priority depends on the layer of the item configured in the qualifier, with layer-4 having a higher priority than layer-3, and layer-3 having a higher priority than layer-2.
Log	Click the **Log** check box to record the number of matched packets in a particular time interval.
Count	Click the **Count** check box to have the Switch count the number of matched packets.
Tme Range	You must have configured a time range in the **Time Range** screen first. Select the name of the time range rule from the drop-down list box to apply a time range to the Classifier rule.
Ingress Port	
Port	Choose **Any** for all ports or enter the ports manually to have the Switch apply the Classifier rule on the ports.
Trunk	Choose **Any** for all trunks or enter the trunks manually to have the Switch apply the Classifier rule on the trunks.
Packet Format	Specify the format of the packet. Choices are **All**, **802.3 tagged**, **802.3 untagged**, **Ethernet II tagged** and **Ethernet II untagged**. A value of **802.3** indicates that the packets are formatted according to the IEEE 802.3 standards. A value of **Ethernet II** indicates that the packets are formatted according to RFC 894, Ethernet II encapsulation.
Layer 2 Specify the fields below to configure a layer-2 classifier.	
VLAN	Select **Any** to classify traffic from any VLAN or select the second option and specify the source VLAN ID in the field provided.
Priority	Select **Any** to classify traffic from any priority level or select the second option and specify a priority level in the field provided.
Ethernet Type	Select an Ethernet type or select **Others** and enter the Ethernet type number in hexadecimal value. Refer to Table 73 on page 167 for information.
Source	
MAC Address	Select **Any** to apply the rule to all MAC addresses. To specify a source, select the MAC buttonand type a MAC address in valid MAC address format (six hexadecimal character pairs).
Mask	Manually type the source MAC mask to which the rule should be applied. You may choose one MAC mask only or all masks (**Any**).
Destination	
MAC Address	Select **Any** to apply the rule to all MAC addresses. To specify a destination, select the second choice and type a MAC address in valid MAC address format (six hexadecimal character pairs).
Mask	Manually type the source MAC mask to which the rule should be applied. You may choose one MAC mask only or all masks (**Any**).
Layer 3 Specify the fields below to configure a layer-3 classifier.	

Table 71 Advanced Application > Classifier > Classifier Configuration (continued)

LABEL	DESCRIPTION
IP Packet Length	Click **Any** to classify any size of packet length or manually enter a range of number (from/to) of packet size in the field provided.
DSCP	Select **Any** to classify traffic from any DSCP or select the second option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided.
Precedence	Click **Any** to classify all packet precedence or select the second option and specify a precedence level in the field provided.
ToS	Click **Any** to classify all ToS (Type of Service) or select the second option and specify a ToS level in the field provided.
IP Protocol	Select an IPv4 protocol type or select **Other** and enter the protocol number in decimal value. Refer to Table 75 on page 168 for more information. You may select **Establish Only** for **TCP** protocol type. This means that the Switch will identify packets that initiate or acknowledge (establish) TCP connections.
IPv6 Next Header	Select an IPv6 protocol type or select **Other** and enter an 8-bit next header in the IPv6 packet. The Next Header field is similar to the IPv4 Protocol field. The IPv6 protocol number ranges from 1 to 255. You may select **Establish Only** for **TCP** protocol type. This means that the Switch will identify packets that initiate or acknowledge (establish) TCP connections.
Source	
IP Address/ Address Prefix	Enter a source IP address in dotted decimal notation. Specify the address prefix by entering the number of ones in the subnet mask.
	Note: You must select either **UDP** or **TCP** in the **IP Protocol** field before you configure the socket numbers. Select **Any** to apply the rule to all TCP/UDP protocol port numbers or select the second option and enter a TCP/UDP protocol port number.
Destination	
IP Address/ Address Prefix	Enter a destination IP address in dotted decimal notation. Specify the address prefix by entering the number of ones in the subnet mask.
Layer 4 Specify the fields below to configure a layer-3 classifier.	
Source/ Destination Socket Number	Note: You must select either **UDP** or **TCP** in the **IP Protocol** field before you configure the socket numbers. Select **Any** to apply the rule to all TCP/UDP protocol port numbers or select the second option and enter a TCP/UDP protocol port number.
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to set the above fields back to the factory defaults.

21.3.1 Viewing and Editing Classifier Configuration

To view a summary of the classifier configuration, scroll down to the summary table at the bottom of the **Classifier** Configuration screen. To change the settings of a rule, click a number in the **Index** field.

Note: When two rules conflict with each other, a higher layer rule has priority over lower layer rule.

Figure 118 Advanced Application > Classifier: Summary Table

The following table describes the labels in this screen.

Table 72 Classifier Status: Summary Table

LABEL	DESCRIPTION
Index	This field displays the index number of the rule. Click an index number to edit the rule.
Active	This field displays **Yes** when the rule is activated and **No** when it is deactivated.
Name	This field displays the descriptive name for this rule. This is for identification purpose only.
Rule	This field displays a summary of the classifier rule's settings.
Delete	Select the classifier rules you want to delete.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

The following table shows some other common Ethernet types and the corresponding protocol number.

Table 73 Common Ethernet Types and Protocol Numbers

ETHERNET TYPE	PROTOCOL NUMBER
IP ETHII	0800
X.75 Internet	0801
NBS Internet	0802
ECMA Internet	0803
Chaosnet	0804
X.25 Level 3	0805
XNS Compat	0807
Banyan Systems	0BAD
BBN Simnet	5208
IBM SNA	80D5
AppleTalk AARP	80F3

In the Internet Protocol there is a field, called “Protocol”, to identify the next level protocol. The following table shows some common protocol types and the corresponding protocol number. Refer to http://www.iana.org/assignments/protocol-numbers for a complete list.

Table 74 Common IP Protocol Types and Protocol Numbers

PROTOCOL TYPE	PROTOCOL NUMBER
ICMP	1
TCP	6
UDP	17
EGP	8
L2TP	115

Some of the most common TCP and UDP port numbers are:

Table 75 Common TCP and UDP Port Numbers

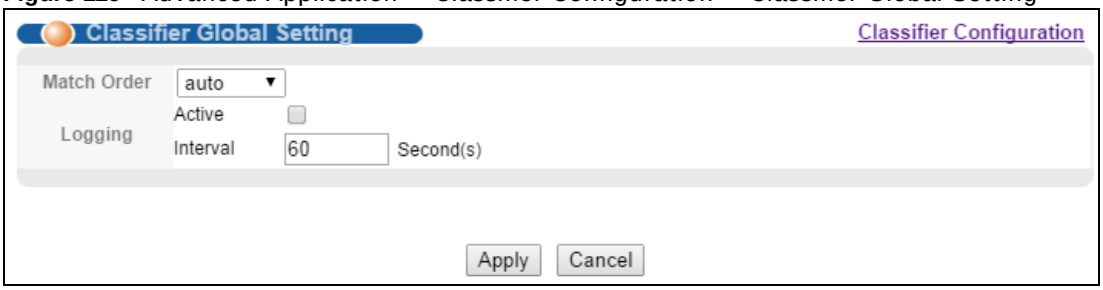
PROTOCOL NAME	TCP/UDP PORT NUMBER
FTP	21
SMTP	25
DNS	53
HTTP	80
POP3	110

See Appendix B on page 379 for information on commonly used port numbers.

21.3.2 Classifier Global Setting

Click **Classifier Global Setting** in the **Classifier Configuration** screen to display the configuration screen as shown.

Figure 119 Advanced Application > Classifier Configuration > Classifier Global Setting



The following table describes the labels in this screen.

Table 76 Advanced Application > Classifier Configuration > Classifier Global Setting

LABEL	DESCRIPTION
Match Order	Select **manual** to have classifier rules applied according to the weight of each rule you configured in **Advanced Application** > **Classifier Configuration**. Alternatively, select **auto** to have classifier rules applied according to the layer of the item configured in the rule. Layer-4 items have the highest priority.
Logging	
Active	Select this to create a log when packets match a classifier rule during a defined time interval.

Table 76 Advanced Application > Classifier Configuration > Classifier Global Setting

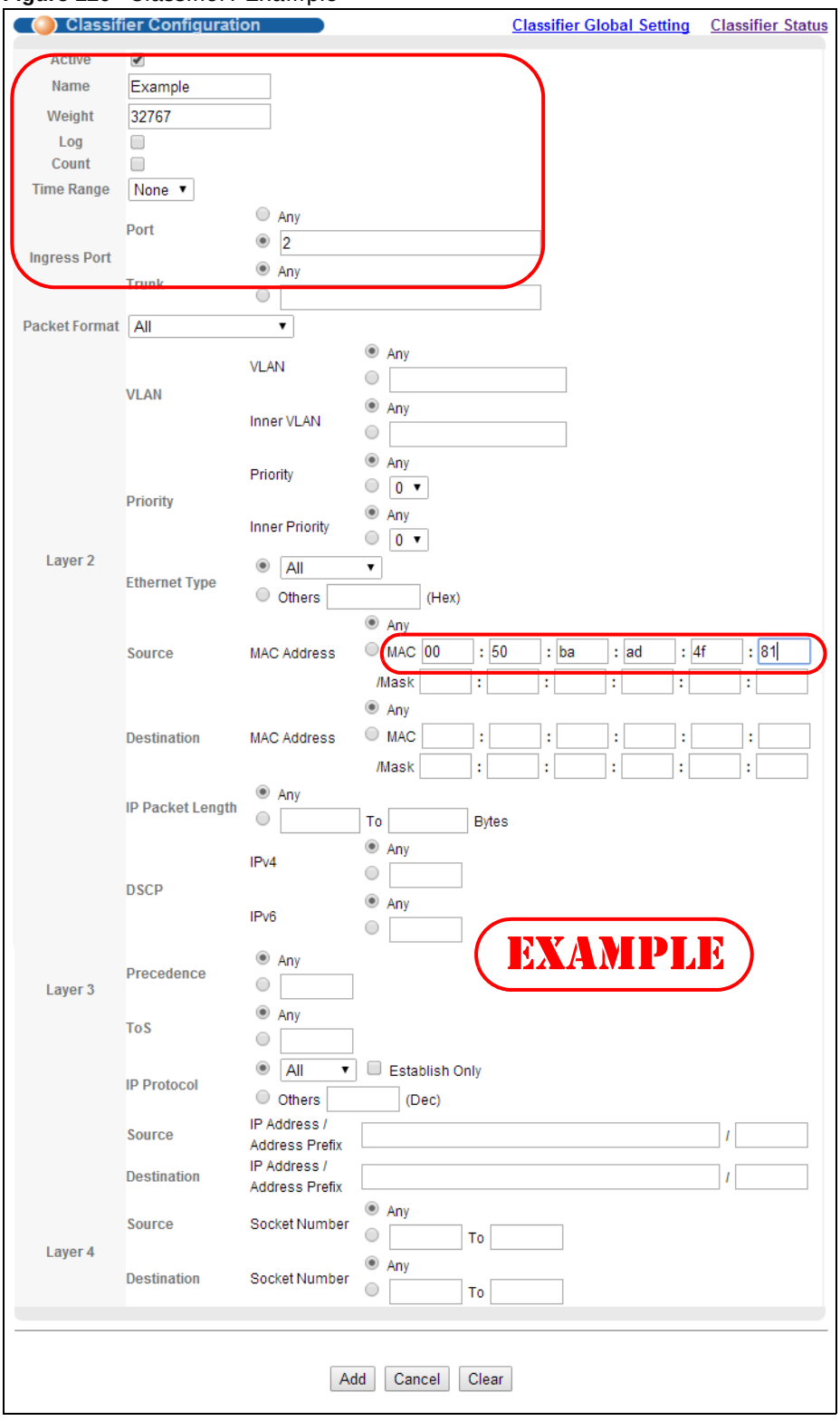
LABEL	DESCRIPTION
Interval	Select the length of the time period (in seconds) to count matched packets for a classifier rule. Enter an integer from 0-65535. 0 means that no logging is done.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

21.4 Classifier Example

The following screen shows an example where you configure a classifier that identifies all traffic from MAC address 00:50:ba:ad:4f:81 on port 2.

After you have configured a classifier, you can configure a policy (in the **Policy** screen) to define action(s) on the classified traffic flow.

Figure 120 Classifier: Example



22

Policy Rule

22.1 Policy Rules Overview

This chapter shows you how to configure policy rules.

A classifier distinguishes traffic into flows based on the configured criteria (refer to Chapter 21 on page 162 for more information). A policy rule ensures that a traffic flow gets the requested treatment in the network.

22.1.1 What You Can Do

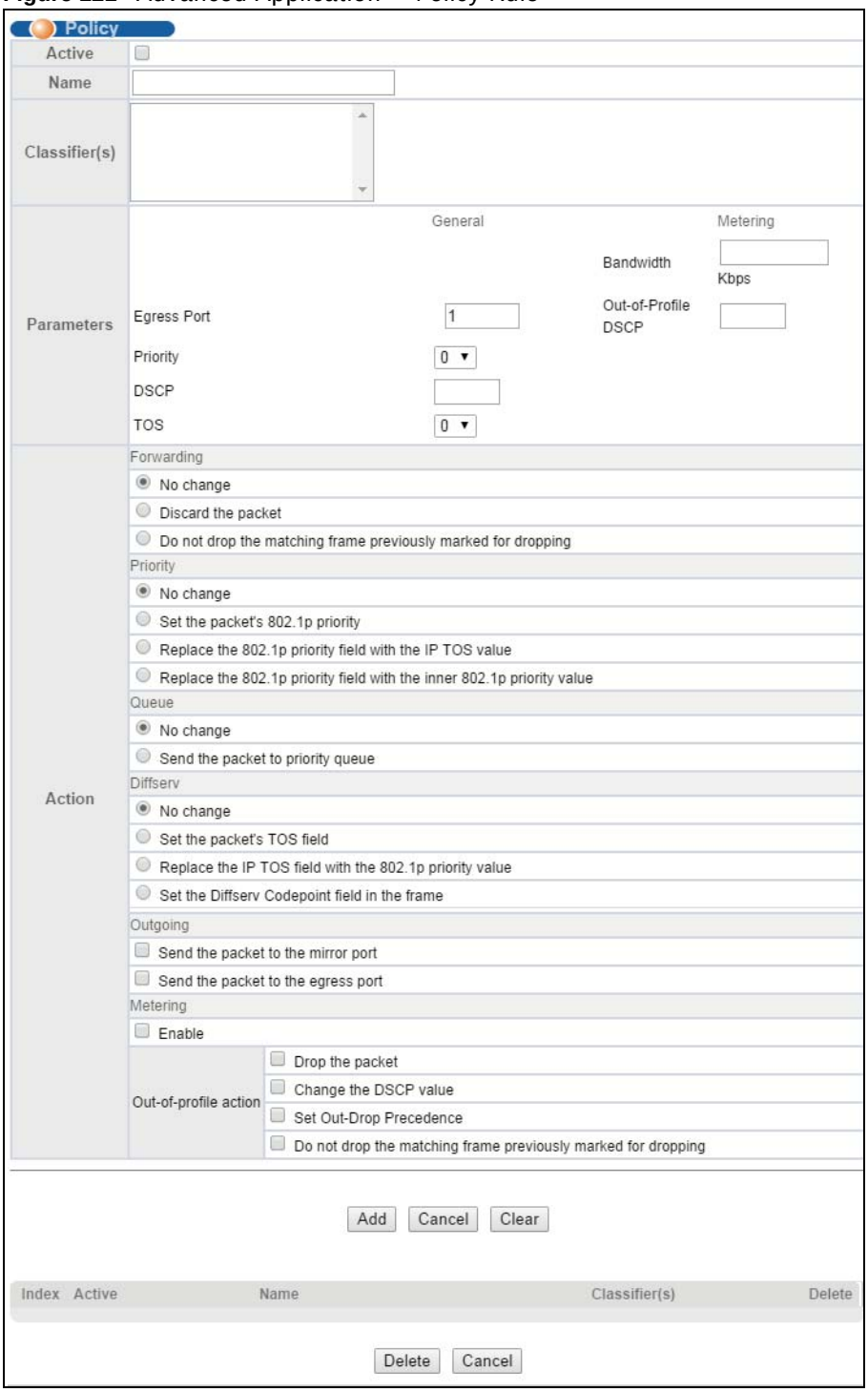
Use the **Policy** screen (Section 22.2 on page 171) to enable the policy and display the active classifier(s) you configure in the **Classifier** screen.

22.2 Configuring Policy Rules

You must first configure a classifier in the **Classifier** screen. Refer to Section 21.2 on page 162 for more information.

Click **Advanced Applications** > **Policy Rule** in the navigation panel to display the screen as shown.

Figure 121 Advanced Application > Policy Rule



The following table describes the labels in this screen.

Table 77 Advanced Application > Policy Rule

LABEL	DESCRIPTION
Active	Select this option to enable the policy.
Name	Enter a descriptive name for identification purposes.

Table 77 Advanced Application > Policy Rule (continued)

LABEL	DESCRIPTION
Classifier(s)	This field displays the active classifier(s) you configure in the **Classifier** screen. Select the classifier(s) to which this policy rule applies. To select more than one classifier, press [SHIFT] and select the choices at the same time.
Parameters Set the fields below for this policy. You only have to set the field(s) that is related to the action(s) you configure in the **Action** field.	
General	
Egress Port	Type the number of an outgoing port.
Priority	Specify a priority level.
DSCP	Specify a DSCP (DiffServ Code Point) number between 0 and 63.
TOS	Specify the type of service (TOS) priority level.
Metering	You can configure the desired bandwidth available to a traffic flow. Traffic that exceeds the maximum bandwidth allocated (in cases where the network is congested) is called out-of-profile traffic.
Bandwidth	Specify the bandwidth in kilobit per second (Kbps). Enter a number between 64 and 1000000.
Out-of-Profile DSCP	Specify a new DSCP number (between 0 and 63) if you want to replace or remark the DSCP number for out-of-profile traffic.
Action Specify the action(s) the Switch takes on the associated classified traffic flow. Note: You can specify only one action (pair) in a policy rule. To have the Switch take multiple actions on the same traffic flow, you need to define multiple classifiers with the same criteria and apply different policy rules.	
Forwarding	Select **No change** to forward the packets. Select **Discard the packet** to drop the packets. Select **Do not drop the matching frame previously marked for dropping** to retain the frames that were marked to be dropped before.
Priority	Select **No change** to keep the priority setting of the frames. Select **Set the packet's 802.1 priority** to replace the frame's 802.1 priority field with the value you set in the Priority field. Select **Replace the 802.1p priority field with the IP TOS value** to replace the frame's 802.1 priority field with the value you set in the TOS field. Select **Replace the 802.1p priority field with the inner 802.1p priority value** to replace the frame's 802.1 priority field with the inner value.
Queue	Select **No change** to keep the frames in the same queue. Select **Send the packet to priority queue** to put the frames in the designated queue.

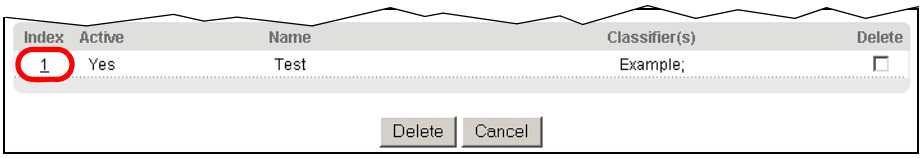
Table 77 Advanced Application > Policy Rule (continued)

LABEL	DESCRIPTION
Diffserv	Select **No change** to keep the TOS and/or DSCP fields in the packets. Select **Set the packet's TOS field** to set the TOS field with the value you configure in the **TOS** field. Select **Replace the IP TOS with the 802.1p priority value** to replace the TOS field with the value you configure in the **Priority** field. Select **Set the Diffserv Codepoint field in the frame** to set the DSCP field with the value you configure in the **DSCP** field.
Outgoing	Select **Send the packet to the mirror port** to send the packet to the mirror port. Select **Send the packet to the egress port** to send the packet to the egress port.
Metering	Select **Enable** to activate bandwidth limitation on the traffic flow(s) then set the actions to be taken on out-of-profile packets.
Out-of-profile action	Select the action(s) to be performed for out-of-profile traffic. Select **Drop the packet** to discard the out-of-profile traffic. Select **Change the DSCP value** to replace the DSCP field with the value specified in the **Out of profile DSCP** field. Select **Set Out-Drop Precedence** to mark out-of-profile traffic and drop it when network is congested. Select **Do not drop the matching frame previously marked for dropping** to queue the frames that are marked to be dropped.
Add	Click **Add** to inset the entry to the summary table below and save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields back to your previous configuration.
Clear	Click **Clear** to set the above fields back to the factory defaults.
Summary Table	
Index	This field displays the policy index number. Click an index number to edit the policy.
Active	This field displays **Yes** when policy is activated and **No** when is it deactivated.
Name	This field displays the name you have assigned to this policy.
Classifier(s)	This field displays the name(s) of the classifier to which this policy applies.
Delete	Click **Delete** to remove the selected entry from the summary table.
Delete	Click **Cancel** to clear the **Delete** check boxes.
Cancel	This field displays the policy index number. Click an index number to edit the policy.

22.2.1 Viewing and Editing Policy Configuration

To view a summary of the classifier configuration, scroll down to the summary table at the bottom of the **Policy** screen. To change the settings of a rule, click a number in the **Index** field.

Figure 122 Advanced Application > Policy Rule: Summary Table



23

Queuing Method

23.1 Queuing Method Overview

This chapter introduces the queuing methods supported.

Queuing is used to help solve performance degradation when there is network congestion. Use the **Queuing Method** screen to configure queuing algorithms for outgoing traffic. See also **Priority Queue Assignment** in **Switch Setup** and **802.1p Priority** in **Port Setup** for related information.

23.1.1 What You Can Do

Use the **Queueing Method** screen (Section 23.2 on page 176) set priorities for the queues of the Switch. This distributes bandwidth across the different traffic queues.

23.1.2 What You Need to Know

Queuing algorithms allow switches to maintain separate queues for packets from each individual source or flow and prevent a source from monopolizing the bandwidth.

Strictly Priority Queuing

Strictly Priority Queuing (SPQ) services queues based on priority only. As traffic comes into the Switch, traffic on the highest priority queue, Q7 is transmitted first. When that queue empties, traffic on the next highest-priority queue, Q6 is transmitted until Q6 empties, and then traffic is transmitted on Q5 and so on. If higher priority queues never empty, then traffic on lower priority queues never gets sent. SPQ does not automatically adapt to changing network requirements.

Weighted Fair Queuing

Weighted Fair Queuing is used to guarantee each queue's minimum bandwidth based on its bandwidth weight (portion) (the number you configure in the Weight field) when there is traffic congestion. WFQ is activated only when a port has more traffic than it can handle. Queues with larger weights get more guaranteed bandwidth than queues with smaller weights. This queuing mechanism is highly efficient in that it divides any available bandwidth across the different traffic queues. By default, the weight for Q0 is 1, for Q1 is 2, for Q2 is 3, and so on.

Weighted Round Robin Scheduling (WRR)

Round Robin Scheduling services queues on a rotating basis and is activated only when a port has more traffic than it can handle. A queue is a given an amount of bandwidth irrespective of the incoming traffic on that port. This queue then moves to the back of the list. The next queue is given

an equal amount of bandwidth, and then moves to the end of the list; and so on, depending on the number of queues being used. This works in a looping fashion until a queue is empty.

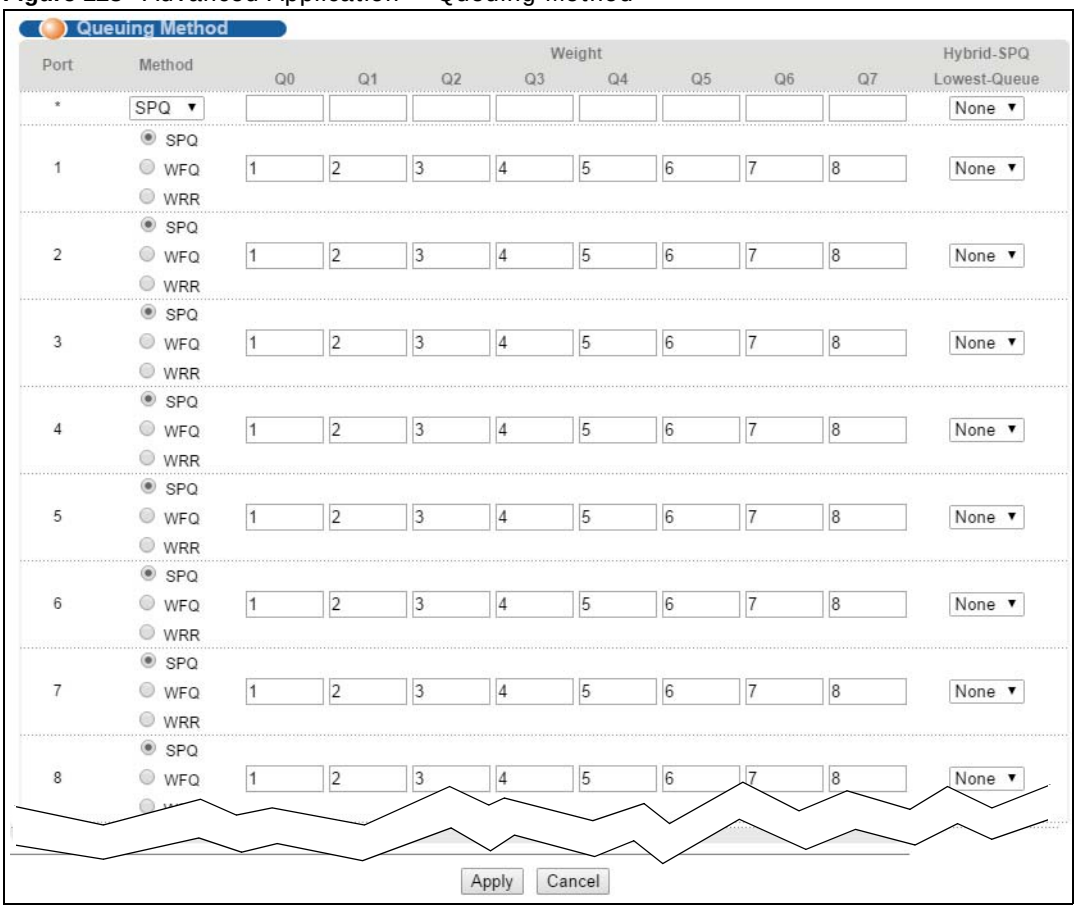
Weighted Round Robin Scheduling (WRR) uses the same algorithm as round robin scheduling, but services queues based on their priority and queue weight (the number you configure in the queue **Weight** field) rather than a fixed amount of bandwidth. WRR is activated only when a port has more traffic than it can handle. Queues with larger weights get more service than queues with smaller weights. This queuing mechanism is highly efficient in that it divides any available bandwidth across the different traffic queues and returns to queues that have not yet emptied.

23.2 Configuring Queuing

Use this screen to set priorities for the queues of the Switch. This distributes bandwidth across the different traffic queues.

Click **Advanced Application** > **Queuing Method** in the navigation panel.

Figure 123 Advanced Application > Queuing Method



The following table describes the labels in this screen.

Table 78 Advanced Application > Queuing Method

LABEL	DESCRIPTION
Port	This label shows the port you are configuring.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Method	Select **SPQ** (Strictly Priority Queuing), **WFQ** (Weighted Fair Queuing) or **WRR** (Weighted Round Robin). Strictly Priority Queuing services queues based on priority only. When the highest priority queue empties, traffic on the next highest-priority queue begins. Q7 has the highest priority and Q0 the lowest. Weighted Fair Queuing is used to guarantee each queue's minimum bandwidth based on their bandwidth portion (weight) (the number you configure in the **Weight** field). Queues with larger weights get more guaranteed bandwidth than queues with smaller weights. Weighted Round Robin Scheduling services queues on a rotating basis based on their queue weight (the number you configure in the queue **Weight** field). Queues with larger weights get more service than queues with smaller weights.
Weight	When you select **WFQ** or **WRR** enter the queue weight here. Bandwidth is divided across the different traffic queues according to their weights.
Hybrid-SPQ Lowest-Queue	This field is applicable only when you select **WFQ** or **WRR**. Select a queue (**Q0** to **Q7**) to have the Switch use **SPQ** to service the subsequent queue(s) after and including the specified queue for the port. For example, if you select **Q5**, the Switch services traffic on **Q5**, **Q6** and **Q7** using **SPQ**. Select **None** to always use **WFQ** or **WRR** for the port.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

24

Multicast

24.1 Multicast Overview

This chapter shows you how to configure various multicast features.

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender to 1 recipient) or Broadcast (1 sender to everybody on the network). Multicast delivers IP packets to just a group of hosts on the network.

IGMP (Internet Group Management Protocol) is a network-layer protocol used to establish membership in a multicast group - it is not used to carry user data. Refer to RFC 1112, RFC 2236 and RFC 3376 for information on IGMP versions 1, 2 and 3 respectively.

24.1.1 What You Can Do

- Use the **Multicast Setup** screen (Section 24.2 on page 182) to enable IGMP snooping to forward group multicast traffic only to ports that are members of that group.
- Use the **IPv4 Multicast Status** screen (Section 24.3 on page 182) to view multicast group information.
- Use the **IPv6 Multicast Status** screen (Section 24.5 on page 188) to view multicast group information.
- Use the **MLD Snooping-proxy** screen (Section 24.5.1 on page 189) to enable the upstream port to report group changes to a connected multicast router and forward MLD messages to other upstream ports. See Section 24.1 on page 178 for more information on multicasting
- Use the **MVR** screens (Section 24.5 on page 188) to create multicast VLANs and select the receiver port(s) and a source port for each multicast VLAN.

24.1.2 What You Need to Know

Read on for concepts on Multicasting that can help you configure the screens in this chapter.

IP Multicast Addresses

In IPv4, a multicast address allows a device to send packets to a specific group of hosts (multicast group) in a different subnetwork. A multicast IP address represents a traffic receiving group, not individual receiving devices. IP addresses in the Class D range (224.0.0.0 to 239.255.255.255) are used for IP multicasting. Certain IP multicast numbers are reserved by IANA for special purposes (see the IANA website for more information).

IGMP Snooping

A Switch can passively snoop on IGMP packets transferred between IP multicast routers/switches and IP multicast hosts to learn the IP multicast group membership. It checks IGMP packets passing

through it, picks out the group registration information, and configures multicasting accordingly. IGMP snooping allows the Switch to learn multicast groups without you having to manually configure them.

The Switch forwards multicast traffic destined for multicast groups (that it has learned from IGMP snooping or that you have manually configured) to ports that are members of that group. IGMP snooping generates no additional network traffic, allowing you to significantly reduce multicast traffic passing through your Switch.

IGMP Snooping and VLANs

The Switch can perform IGMP snooping on up to 16 VLANs. You can configure the Switch to automatically learn multicast group membership of any VLANs. The Switch then performs IGMP snooping on the first 16 VLANs that send IGMP packets. This is referred to as auto mode. Alternatively, you can specify the VLANs that IGMP snooping should be performed on. This is referred to as fixed mode. In fixed mode the Switch does not learn multicast group membership of any VLANs other than those explicitly added as an IGMP snooping VLAN.

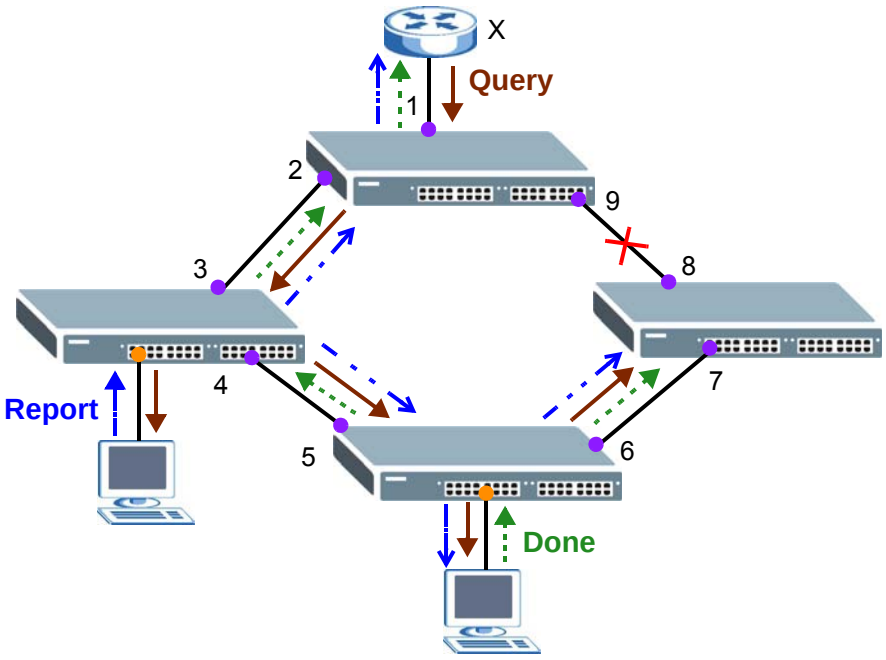
MLD Snooping-proxy

MLD snooping-proxy is a ZyXEL-proprietary feature. IPv6 MLD proxy allows only one upstream interface on a switch, while MLD snooping-proxy supports more than one upstream port on a switch. The upstream port in MLD snooping-proxy can report group changes to a connected multicast router and forward MLD messages to other upstream ports. This helps especially when you want to have a network that uses STP to provide backup links between switches and also performs MLD snooping and proxy functions. MLD snooping-proxy, like MLD proxy, can minimize MLD control messages and allow better network performance.

In MLD snooping-proxy, if one upstream port is learned via snooping, all other upstream ports on the same device will be added to the same group. If one upstream port requests to leave a group, all other upstream ports on the same device will also be removed from the group.

In the following MLD snooping-proxy example, all connected upstream ports (1 ~7) are treated as one interface. The connection between ports 8 and 9 is blocked by STP to break the loop. If there is

one query from a router (**X**) or MLD Done or Report message from any upstream port, it will be broadcast to all connected upstream ports.



MLD Messages

A multicast router or switch periodically sends general queries to MLD hosts to update the multicast forwarding table. When an MLD host wants to join a multicast group, it sends an MLD Report message for that address.

An MLD Done message is similar to an IGMP Leave message. When an MLD host wants to leave a multicast group, it can send a Done message to the router or switch. If the leave mode is not set to **Immediate**, the router or switch sends a group-specific query to the port on which the Done message is received to determine if other devices connected to this port should remain in the group.

MVR Overview

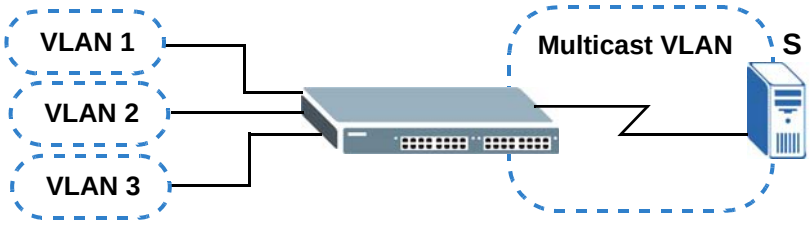
Multicast VLAN Registration (MVR) is designed for applications (such as Media-on-Demand (MoD)) that use multicast traffic across an Ethernet ring-based service provider network.

MVR allows one single multicast VLAN to be shared among different subscriber VLANs on the network. While isolated in different subscriber VLANs, connected devices can subscribe to and unsubscribe from the multicast stream in the multicast VLAN. This improves bandwidth utilization with reduced multicast traffic in the subscriber VLANs and simplifies multicast group management.

MVR only responds to IGMP join and leave control messages from multicast groups that are configured under MVR. Join and leave reports from other multicast groups are managed by IGMP snooping.

The following figure shows a network example. The subscriber VLAN (**1**, **2** and **3**) information is hidden from the streaming media server, **S**. In addition, the multicast VLAN information is only visible to the Switch and **S**.

Figure 124 MVR Network Example



Types of MVR Ports

In MVR, a source port is a port on the Switch that can send and receive multicast traffic in a multicast VLAN while a receiver port can only receive multicast traffic. Once configured, the Switch maintains a forwarding table that matches the multicast stream to the associated multicast group.

MVR Modes

You can set your Switch to operate in either dynamic or compatible mode.

In dynamic mode, the Switch sends IGMP leave and join reports to the other multicast devices (such as multicast routers or servers) in the multicast VLAN. This allows the multicast devices to update the multicast forwarding table to forward or not forward multicast traffic to the receiver ports.

In compatible mode, the Switch does not send any IGMP reports. In this case, you must manually configure the forwarding settings on the multicast devices in the multicast VLAN.

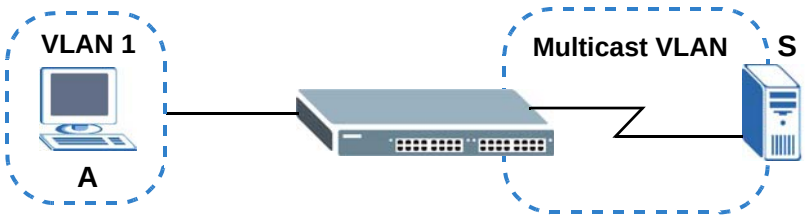
How MVR Works

The following figure shows a multicast television example where a subscriber device (such as a computer) in VLAN 1 receives multicast traffic from the streaming media server, **S**, via the Switch. Multiple subscriber devices can connect through a port configured as the receiver on the Switch.

When the subscriber selects a television channel, computer **A** sends an IGMP report to the Switch to join the appropriate multicast group. If the IGMP report matches one of the configured MVR multicast group addresses on the Switch, an entry is created in the forwarding table on the Switch. This maps the subscriber VLAN to the list of forwarding destinations for the specified multicast traffic.

When the subscriber changes the channel or turns off the computer, an IGMP leave message is sent to the Switch to leave the multicast group. The Switch sends a query to VLAN 1 on the receiver port (in this case, an uplink port on the Switch). If there is another subscriber device connected to this port in the same subscriber VLAN, the receiving port will still be on the list of forwarding destination for the multicast traffic. Otherwise, the Switch removes the receiver port from the forwarding table.

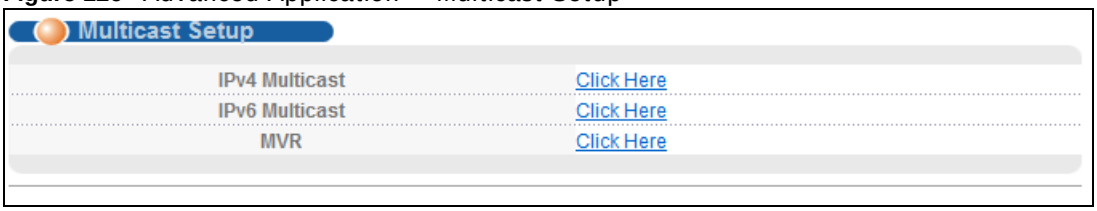
Figure 125 MVR Multicast Television Example



24.2 Multicast Setup

Use this screen to configure IGMP for IPv4 or MLD for IPv6 and set up multicast VLANs. Click **Advanced Application** > **Multicast** in the navigation panel.

Figure 126 Advanced Application > Multicast Setup



The following table describes the labels in this screen.

Table 79 Advanced Application > Multicast Setup

LABEL	DESCRIPTION
IPv4 Multicast	Click the link to open screens where you can configure IGMP snooping and IGMP filtering for IPv4.
IPv6 Multicast	Click the link to open screens where you can configure MLD snooping and MLD filtering for IPv6.
MVR	Click the link to open screens where you can create multicast VLANs.

24.3 IPv4 Multicast Status

Click **Advanced Application > Multicast > IPv4 Multicast** to display the screen as shown. This screen shows the IPv4 multicast group information. See Section 24.1 on page 178 for more information on multicasting.

Figure 127 Advanced Application > Multicast > IPv4 Multicast

The following table describes the labels in this screen.

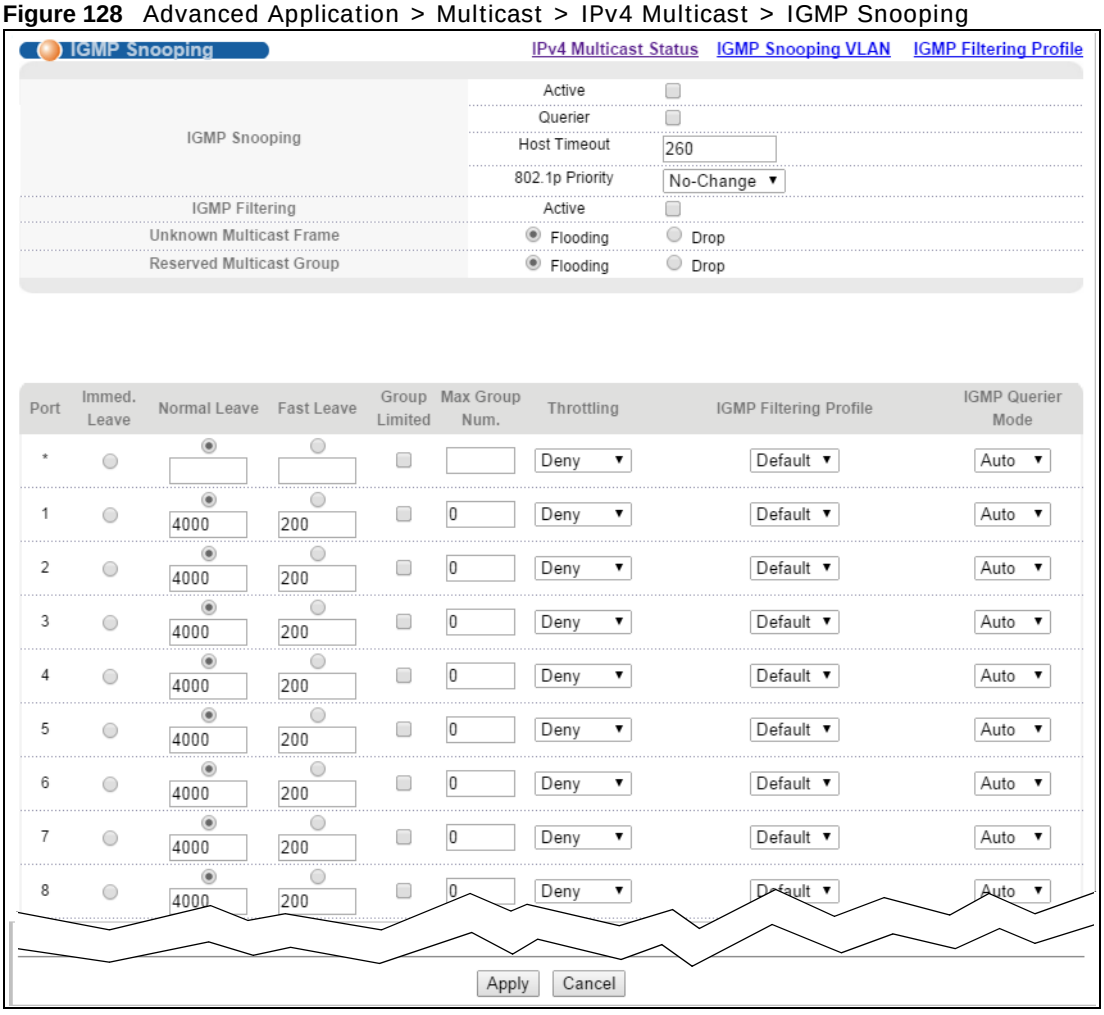
Table 80 Advanced Application > Multicast > IPv4 Multicast

LABEL	DESCRIPTION
Index	This is the index number of the entry.
VID	This field displays the multicast VLAN ID.
Port	This field displays the port number that belongs to the multicast group.
Multicast Group	This field displays IP multicast group addresses.

24.3.1 IGMP Snooping

Click the **IGMP Snooping** link in the **Advanced Application > Multicast > IPv4 Multicast** screen to display the screen as shown. See Section 24.1 on page 178 for more information on multicasting.

Figure 128 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping



The following table describes the labels in this screen.

Table 81 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping

LABEL	DESCRIPTION
IGMP Snooping	Use these settings to configure IGMP snooping.
Active	Select **Active** to enable IGMP Snooping to forward group multicast traffic only to ports that are members of that group.
Querier	Select this option to allow the Switch to send IGMP General Query messages to the VLANs with the multicast hosts attached.
Host Timeout	Specify the time (from 1 to 16 711 450) in seconds that elapses before the Switch removes an IGMP group membership entry if it does not receive report messages from the port.
802.1p Priority	Select a priority level (0-7) to which the Switch changes the priority in outgoing IGMP control packets. Otherwise, select **No-Change** to not replace the priority.
IGMP Filtering	Select **Active** to enable IGMP filtering to control which IGMP groups a subscriber on a port can join. If you enable IGMP filtering, you must create and assign IGMP filtering profiles for the ports that you want to allow to join multicast groups.
Unknown Multicast Frame	Specify the action to perform when the Switch receives an unknown multicast frame. Select **Drop** to discard the frame(s). Select **Flooding** to send the frame(s) to all ports.
Reserved Multicast Group	The IP address range of 224.0.0.0 to 224.0.0.255 are reserved for multicasting on the local network only. For example, 224.0.0.1 is for all hosts on a local network segment and 224.0.0.9 is used to send RIP routing information to all RIP v2 routers on the same network segment. A multicast router will not forward a packet with the destination IP address within this range to other networks. See the IANA web site for more information. The layer-2 multicast MAC addresses used by Cisco layer-2 protocols, 01:00:0C:CC:CC:CC and 01:00:0C:CC:CC:CD, are also included in this group. Specify the action to perform when the Switch receives a frame with a reserved multicast address. Select **Drop** to discard the frame(s). Select **Flooding** to send the frame(s) to all ports.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Changes in this row are copied to all the ports as soon as you make them.
Immed. Leave	Select this option to set the Switch to remove this port from the multicast tree when an IGMP version 2 leave message is received on this port. Select this option if there is only one host connected to this port.
Normal Leave	Enter an IGMP normal leave timeout value (from 200 to 6,348,800) in miliseconds. Select this option to have the Switch use this timeout to update the forwarding table for the port. In normal leave mode, when the Switch receives an IGMP leave message from a host on a port, it forwards the message to the multicast router. The multicast router then sends out an IGMP Group-Specific Query (GSQ) message to determine whether other hosts connected to the port should remain in the specific multicast group. The Switch forwards the query message to all hosts connected to the port and waits for IGMP reports from hosts to update the forwarding table. This defines how many seconds the Switch waits for an IGMP report before removing an IGMP snooping membership entry when an IGMP leave message is received on this port from a host.

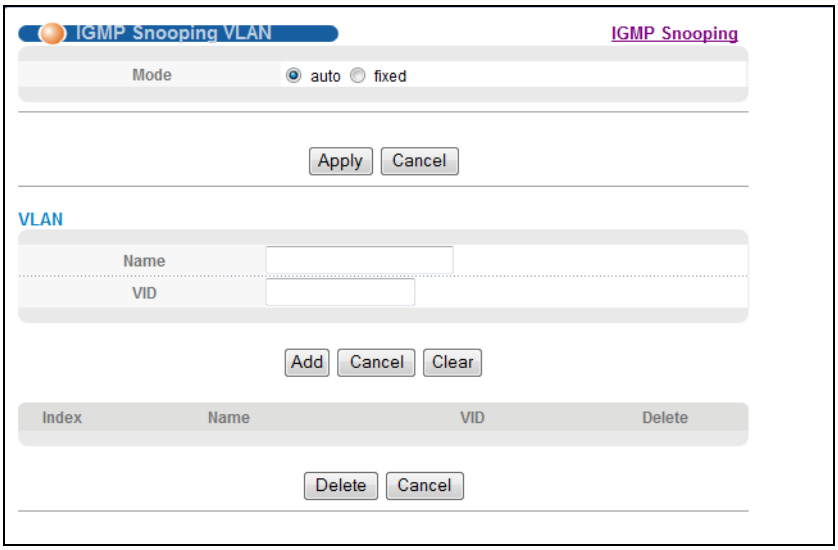
Table 81 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping (continued)

LABEL	DESCRIPTION
Fast Leave	Enter an IGMP fast leave timeout value (from 200 to 6,348,800) in miliseconds. Select this option to have the Switch use this timeout to update the forwarding table for the port. In fast leave mode, right after receiving an IGMP leave message from a host on a port, the Switch itself sends out an IGMP Group-Specific Query (GSQ) message to determine whether other hosts connected to the port should remain in the specific multicast group. This helps speed up the leave process. This defines how many seconds the Switch waits for an IGMP report before removing an IGMP snooping membership entry when an IGMP leave message is received on this port from a host.
Group Limited	Select this option to limit the number of multicast groups this port is allowed to join.
Max Group Num.	Enter the number of multicast groups this port is allowed to join. Once a port is registered in the specified number of multicast groups, any new IGMP join report frame(s) is dropped on this port.
Throttling	IGMP throttling controls how the Switch deals with the IGMP reports when the maximum number of the IGMP groups a port can join is reached. Select **Deny** to drop any new IGMP join report received on this port until an existing multicast forwarding table entry is aged out. Select **Replace** to replace an existing entry in the multicast forwarding table with the new IGMP report(s) received on this port.
IGMP Filtering Profile	Select the name of the IGMP filtering profile to use for this port. Otherwise, select **Default** to prohibit the port from joining any multicast group. You can create IGMP filtering profiles in the **Multicast > IPv4 Multicast > IGMP Snooping > IGMP Filtering Profile** screen.
IGMP Querier Mode	The Switch treats an IGMP query port as being connected to an IGMP multicast router (or server). The Switch forwards IGMP join or leave packets to an IGMP query port. Select **Auto** to have the Switch use the port as an IGMP query port if the port receives IGMP query packets. Select **Fixed** to have the Switch always use the port as an IGMP query port. Select this when you connect an IGMP multicast server to the port. Select **Edge** to stop the Switch from using the port as an IGMP query port. The Switch will not keep any record of an IGMP router being connected to this port. The Switch does not forward IGMP join or leave packets to this port.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

24.4 IGMP Snooping VLAN

Click **Advanced Application > Multicast > IPv4 Multicast** in the navigation panel. Click the **IGMP Snooping** link and then the **IGMP Snooping VLAN** link to display the screen as shown. See Section on page 179 for more information on IGMP Snooping VLAN.

Figure 129 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping > IGMP Snooping VLAN



The following table describes the labels in this screen.

Table 82 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping > IGMP Snooping VLAN

LABEL	DESCRIPTION
Mode	Select **auto** to have the Switch learn multicast group membership information of any VLANs automatically. Select **fixed** to have the Switch only learn multicast group membership information of the VLAN(s) that you specify below. In either **auto** or **fixed** mode, the Switch can learn up to 16 VLANs (including up to five VLANs you configured in the **MVR** screen). For example, if you have configured one multicast VLAN in the **MVR** screen, you can only specify up to 15 VLANs in this screen. The Switch drops any IGMP control messages which do not belong to these 16 VLANs. You must also enable IGMP snooping in the **Multicast > IPv4 Multicast > IGMP Snooping** screen first.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
VLAN	Use this section of the screen to add VLANs upon which the Switch is to perform IGMP snooping.
Name	Enter the descriptive name of the VLAN for identification purposes.
VID	Enter the ID of a static VLAN; the valid range is between 1 and 4094. You cannot configure the same VLAN ID as in the **MVR** screen.
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to your previous configuration.
Clear	Click **Clear** to reset the fields to the factory defaults.

Table 82 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping > IGMP Snooping VLAN (continued)

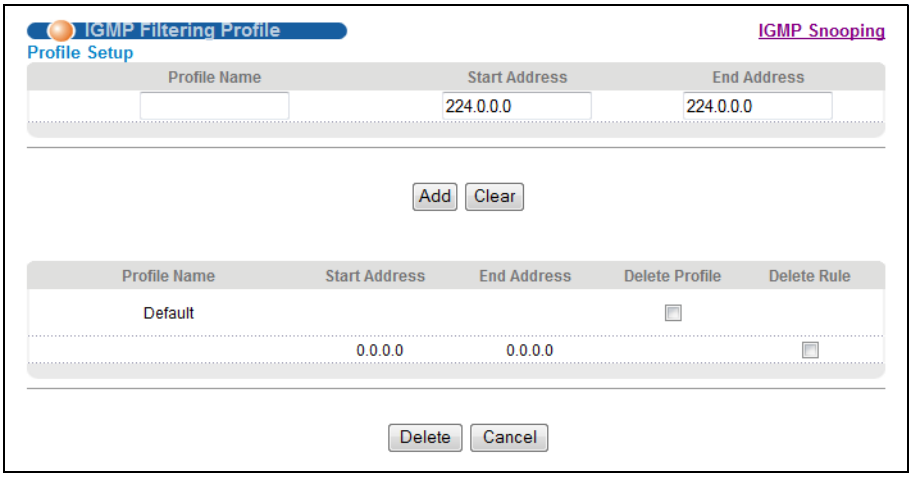
LABEL	DESCRIPTION
Index	This is the index number of the IGMP snooping VLAN entry in the table. Click on an index number to view more details or change the settings.
Name	This field displays the descriptive name for this VLAN group.
VID	This field displays the ID number of the VLAN group.
Delete	Check the entry(ies) that you want to remove in the **Delete** column, then click the **Delete** button.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

24.4.1 IGMP Filtering Profile

An IGMP filtering profile specifies a range of multicast groups that clients connected to the Switch are able to join. A profile contains a range of multicast IP addresses which you want clients to be able to join. Profiles are assigned to ports (in the **IGMP Snooping** screen). Clients connected to those ports are then able to join the multicast groups specified in the profile. Each port can be assigned a single profile. A profile can be assigned to multiple ports.

Click **Advanced Application > Multicast > IPv4 Multicast** in the navigation panel. Click the **IGMP Snooping** link and then the **IGMP Filtering Profile** link to display the screen as shown.

Figure 130 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping > IGMP Filtering Profile



The following table describes the labels in this screen.

Table 83 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping > IGMP Filtering Profile

LABEL	DESCRIPTION
Profile Name	Enter a descriptive name for the profile for identification purposes. To configure additional rule(s) for a profile that you have already added, enter the profile name and specify a different IP multicast address range.
Start Address	Type the starting multicast IP address for a range of multicast IP addresses that you want to belong to the IGMP filter profile.

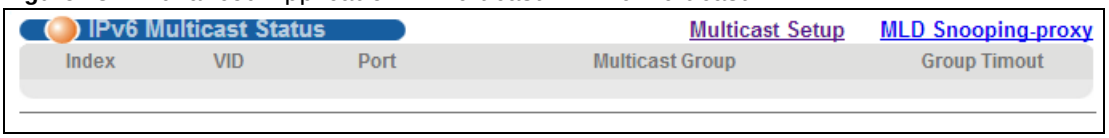
Table 83 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping > IGMP Filtering Profile (continued)

LABEL	DESCRIPTION
End Address	Type the ending multicast IP address for a range of IP addresses that you want to belong to the IGMP filter profile. If you want to add a single multicast IP address, enter it in both the **Start Address** and **End Address** fields.
Add	Click this to create a new entry. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Clear	Click **Clear** to reset the fields to the factory defaults.
Profile Name	This field displays the descriptive name of the profile.
Start Address	This field displays the start of the multicast address range.
End Address	This field displays the end of the multicast address range.
Delete	To delete the profile(s) and all the accompanying rules, select the profile(s) that you want to remove in the **Delete Profile** column, then click the **Delete** button. To delete a rule(s) from a profile, select the rule(s) that you want to remove in the **Delete Rule** column, then click the **Delete** button.
Cancel	Click **Cancel** to clear the **Delete Profile**/**Delete Rule** check boxes.

24.5 IPv6 Multicast Status

Click **Advanced Application > Multicast > IPv6 Multicast** to display the screen as shown. This screen shows the IPv6 multicast group information. See Section 24.1 on page 178 for more information on multicasting.

Figure 131 Advanced Application > Multicast > IPv6 Multicast



The following table describes the fields in the above screen.

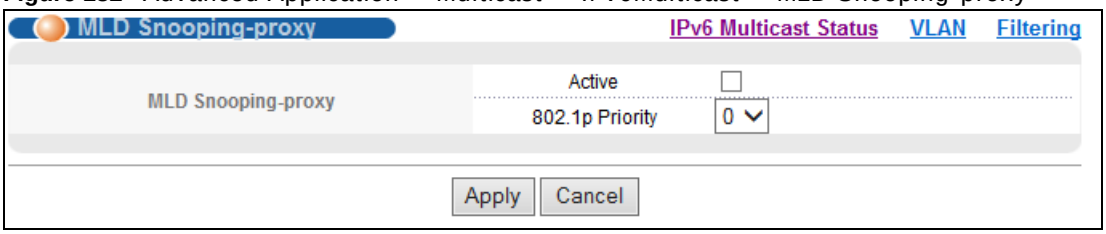
Table 84 Advanced Application > Multicast > IPv6 Multicast

LABEL	DESCRIPTION
Index	This is the index number of the entry.
VID	This field displays the multicast VLAN ID.
Port	This field displays the port number that belongs to the multicast group.
Multicast Group	This field displays IP multicast group addresses.
Group Timout	This field displays the time (in seconds) that elapses before the Switch removes a MLD group membership entry if it does not receive report messages from the port.

24.5.1 MLD Snooping-proxy

Click the **MLD Snooping-proxy** link in the **Advanced Application > Multicast > IPv6 Multicast** screen to display the screen as shown. See Section 24.1 on page 178 for more information on multicasting.

Figure 132 Advanced Application > Multicast > IPv6Multicast > MLD Snooping-proxy



The following tabel describes the fields in the above screen.

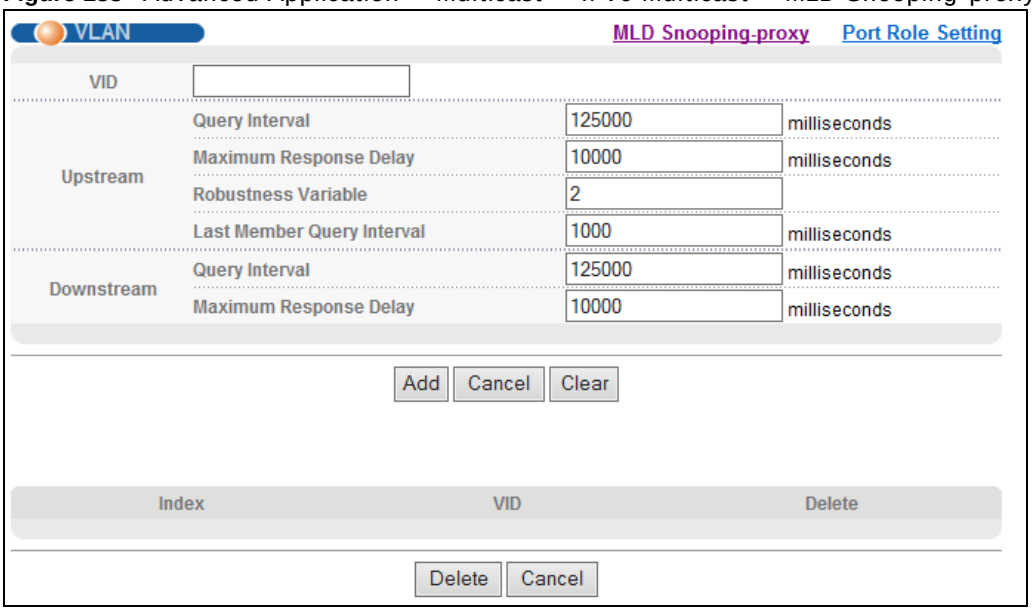
Table 85 Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy

LABEL	DESCRIPTION
MLD Snooping-proxy	Use these settings to configure MLD snooping-proxy.
Active	Select Active to enable MLD snooping-proxy on the Switch to minimize MLD control messages and allow better network performance.
802.1p Priority	Select a priority level (0-7) to which the Switch changes the priority in outgoing MLD messages.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

24.5.2 MLD Snooping-proxy VLAN

Click the **VLAN** link in the **Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy** screen to display the screen as shown.

Figure 133 Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > VLAN



The following table describes the fields in the above screen.

Table 86 Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > VLAN

LABEL	DESCRIPTION
VID	Enter the ID number of the VLAN on which you want to enable MLD snooping-proxy and configure related settings.
Upstream	
Query Interval	Enter the amount of time (in miliseconds) between general query messages sent by the router connected to the upstream port. This value should be exactly the same as what's configured in the connected multicast router. This value is used to calculate the amount of time an MLD snooping membership entry (learned only on the upstream port) can remain in the forwarding table. When an MLD Report message is received, the Switch sets the timeout period of the entry to be T = (QI*RV) + MRD, where T = Timeout, QI = Query Interval, RV = Robustness Variable, and MRD = Maximum Response Delay.
Maximum Response Delay	Enter the amount of time (in miliseconds) the router connected to the upstream port waits for a response to an MLD general query message. This value should be exactly the same as what's configured in the connected multicast router. This value is used to calculate the amount of time an MLD snooping membership entry (learned only on the upstream port) can remain in the forwarding table. When an MLD Report message is received, the Switch sets the timeout period of the entry to be T = (QI*RV) + MRD, where T = Timeout, QI = Query Interval, RV = Robustness Variable, and MRD = Maximum Response Delay. When an MLD Done message is received, the Switch sets the entry's lifetime to be the product of **Last Member Query Interval** and **Robustness Variable**
Robustness Variable	Enter the number of queries. A multicast address entry (learned only on an upstream port by snooping) is removed from the forwarding table when there is no response to the configured number of queries sent by the router connected to the upstream port. This value should be exactly the same as what's configured in the connected multicast router. This value is used to calculate the amount of time an MLD snooping membership entry (learned only on the upstream port) can remain in the forwarding table.

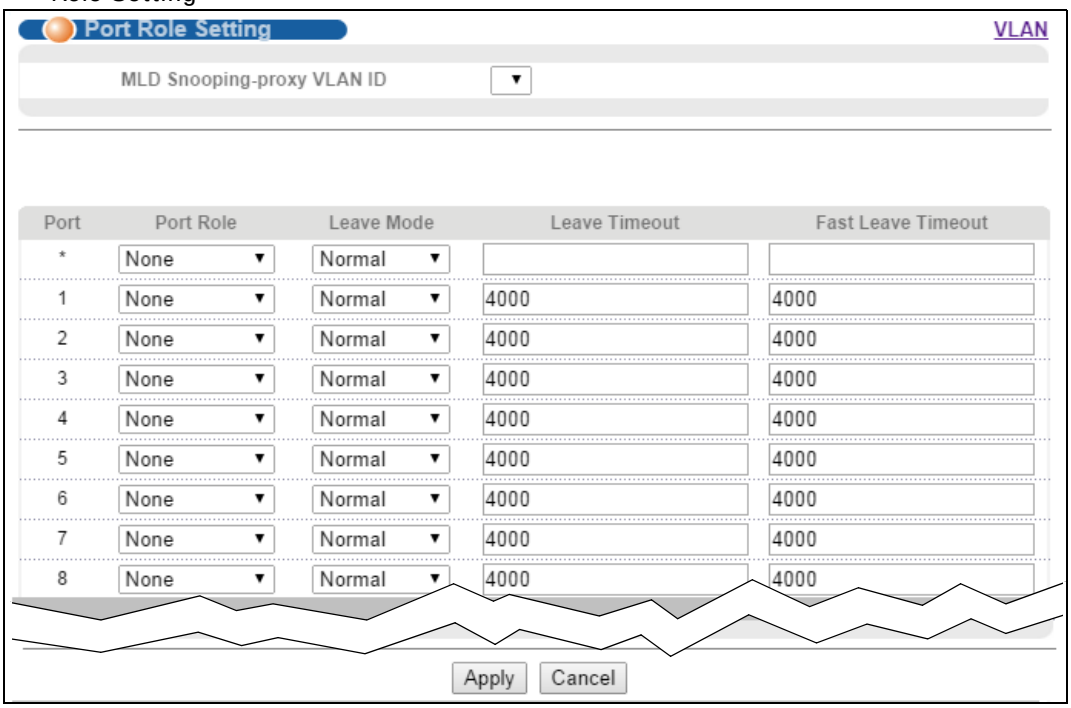
Table 86 Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > VLAN

LABEL	DESCRIPTION
Last Member Query Interval	Enter the amount of time (in miliseconds) between the MLD group-specific queries sent by an upstream port when an MLD Done message is received. This value should be exactly the same as what's configured in the connected multicast router. This value is used to calculate the amount of time an MLD snooping membership entry (learned only on the upstream port) can remain in the forwarding table after a Done message is received. When an MLD Done message is received, the Switch sets the entry's lifetime to be the product of **Last Member Query Interval** and **Robustness Variable.**
Downstream	
Query Interval	Enter the amount of time (in miliseconds) between general query messages sent by the downstream port.
Maximum Response Delay	Enter the maximum time (in miliseconds) that the Switch waits for a response to a general query message sent by the downstream port.
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to your previous configuration.
Clear	Click **Clear** to reset the fields to the factory defaults.
Index	This is the index number of the MLD snooping-proxy VLAN entry in the table. Click on an index number to view more details or change the settings.
VID	This field displays the ID number of the VLAN group.
Delete	Check the entry(ies) that you want to remove in the **Delete** column.
Delete	Click **Delete** to remove the entry selected in the Delete column permanently.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

24.5.3 MLD Snooping-proxy VLAN Port Role Setting

Click the **Port Role Setting** link in the **Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > VLAN** screen to display the screen as shown.

Figure 134 Advanced Applicaton > Multicast > IPv6 Multicast > MLD Snooping-proxy > VLAN > Port Role Setting



The following table describes the fields in the above screen.

Table 87 Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > VLAN > Port Role Setting

LABEL	DESCRIPTION
MLD Snooping-proxy VLAN ID	Select the VLAN ID for which you want to configure a port's MLD snooping-proxy settings.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Changes in this row are copied to all the ports as soon as you make them.
Port Role	A port on the Switch can be either a **Downstream** port or **Upstream** port in MLD. A downstream port connects to MLD hosts and acts as a multicast router to send MLD queries and listen to the MLD host's Report and Done messages. An upstream port connects to a multicast router and works as a host to send Report or Done messages when receiving queries from a multicast router. Otherwise, select **None** if the port is not joining a multicast group or does not belong to this VLAN.
Leave Mode	Select the leave mode for the specified downstream port(s) in this VLAN. This specifies whether the Switch removes an MLD snooping membership entry (learned on a downstream port) immediately (**Immediate**) or wait for an MLD report before the leave timeout (**Normal**) or fast leave timeout (**Fast**) when an MLD leave message is received on this port from a host.

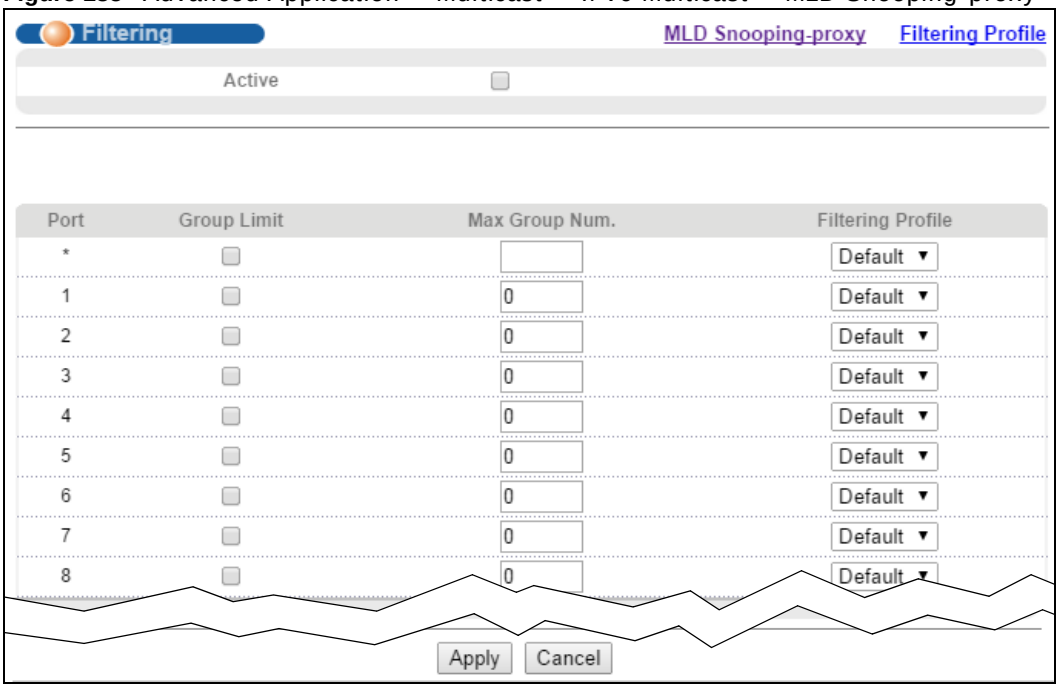
Table 87 Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > VLAN > Port Role Setting

LABEL	DESCRIPTION
Leave Timeout	Enter the MLD snooping normal leave timeout (in milliseconds) the Switch uses to update the forwarding table for the specified downstream port(s). This defines how many seconds the Switch waits for an MLD report before removing an MLD snooping membership entry (learned on a downstream port) when an MLD Done message is received on this port from a host.
Fast Leave Timeout	Enter the fast leave timeout (in milliseconds) for the specified downstream port(s). This defines how many seconds the Switch waits for an MLD report before removing an MLD snooping membership entry (learned on a downstream port) when an MLD Done message is received on this port from a host.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to your previous configuration.

24.5.4 MLD Snooping-proxy VLAN Filtering

Use this screen to configure the Switch's MLD filtering settings. Click the **Filtering** link in the **Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy** screen to display the screen as shown.

Figure 135 Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > Filtering



The following table describes the fields in the above screen.

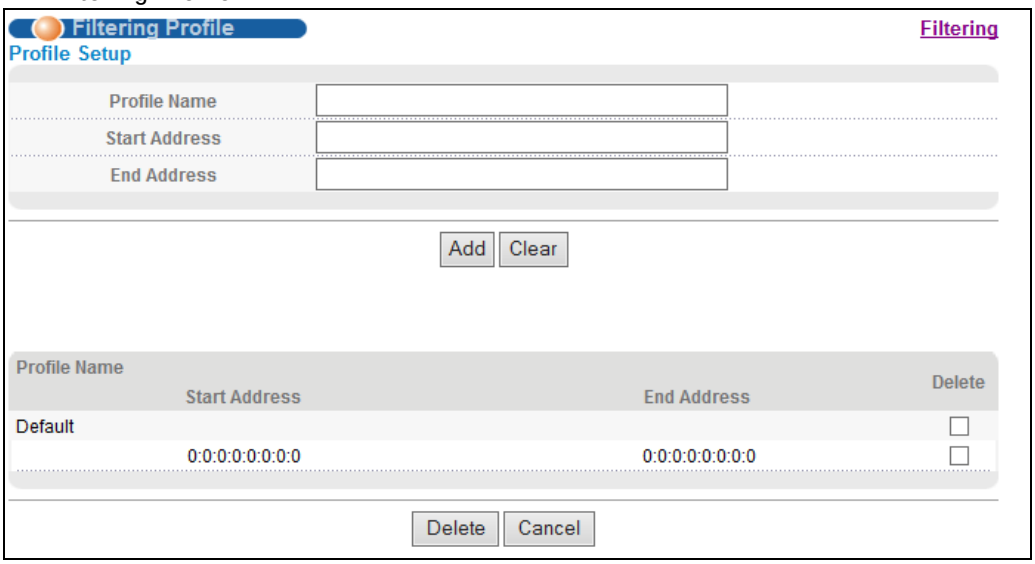
Table 88 Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > Filtering

LABEL	DESCRIPTION
Active	Select this option to enable MLD filtering on the Switch.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Changes in this row are copied to all the ports as soon as you make them.
Group Limit	Select this option to limit the number of multicast groups this port is allowed to join.
Max Group Num.	Enter the number of multicast groups this port is allowed to join. Once a port is registered in the specified number of multicast groups, any new MLD Report message is dropped on this port.
Filtering Profile	Select the name of the MLD filtering profile to use for this port. Otherwise, select **Default** to prohibit the port from joining any multicast group. You can create MLD filtering profiles in the **Multicast > IPv6 Multicast > MLD Snooping-proxy > Filtering > Filtering Profile** screen.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to your previous configuration.

24.5.5 MLD Snooping-proxy VLAN Filtering Profile

Use this screen to create an MLD filtering profile and set the range of the multicast address(es). Click the **Filtering Profile** link in the **Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > Filtering** screen to display the screen as shown.

Figure 136 Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > Filtering > Filtering Profile



The following table describes the fields in the above screen.

Table 89 Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > Filtering Profile

LABEL	DESCRIPTION
Profile Name	Enter a descriptive name for the profile for identification purposes. To configure additional rule(s) for a profile that you have already added, enter the profile name and specify a different IP multicast address range.
Start Address	Type the starting multicast IPv6 address for a range of multicast IPv6 addresses that you want to belong to the MLD filtering profile.
End Address	Type the ending multicast IPv6 address for a range of IPv6 addresses that you want to belong to the MLD filtering profile. If you want to add a single multicast IPv6 address, enter it in both the **Start Address** and **End Address** fields.
Add	Click this to create a new entry. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Clear	Click **Clear** to reset the fields to the factory defaults.
Profile Name	This field displays the descriptive name of the profile.
Start Address	This field displays the start of the multicast IPv6 address range.
End Address	This field displays the end of the multicast IPv6 address range.
Delete	To delete the profile(s) and all the accompanying rules, select the profile(s) that you want to remove in the **Delete Profile** column, then click the **Delete** button. To delete a rule(s) from a profile, select the rule(s) that you want to remove in the **Delete Rule** column, then click the **Delete** button.
Delete	Click **Delte** button to permanently delete the entries you selected in the Delete column.
Cancel	Click **Cancel** to clear the **Delete Profile**/**Delete Rule** check boxes.

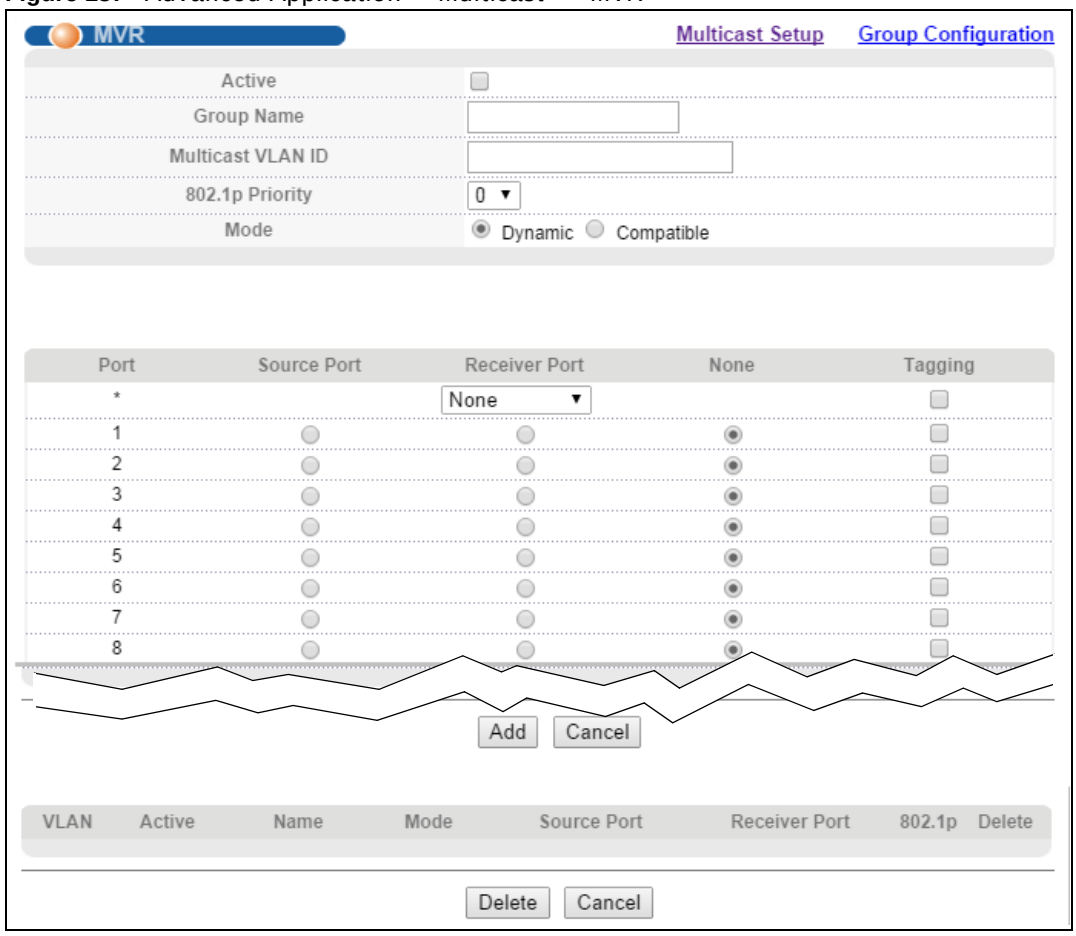
24.6 General MVR Configuration

Use the **MVR** screen to create multicast VLANs and select the receiver port(s) and a source port for each multicast VLAN. Click **Advanced Application > Multicast** > **MVR** to display the screen as shown next.

Note: You can create up to five multicast VLANs and up to 256 multicast rules on the Switch.

Note: Your Switch automatically creates a static VLAN (with the same VID) when you create a multicast VLAN in this screen.

Figure 137 Advanced Application > Multicast > MVR



The following table describes the related labels in this screen.

Table 90 Advanced Application > Multicast > Multicast Setting > MVR

LABEL	DESCRIPTION
Active	Select this check box to enable MVR to allow one single multicast VLAN to be shared among different subscriber VLANs on the network.
Group Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.
Multicast VLAN ID	Enter the VLAN ID (1 to 4094) of the multicast VLAN.
802.1p Priority	Select a priority level (0-7) with which the Switch replaces the priority in outgoing IGMP or MLD control packets (belonging to this multicast VLAN).
Mode	Specify the MVR mode on the Switch. Choices are **Dynamic** and **Compatible**. Select **Dynamic** to send IGMP reports or MLD messages to all MVR source ports in the multicast VLAN. Select **Compatible** to set the Switch not to send IGMP reports or MLD messages.
Port	This field displays the port number on the Switch.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Changes in this row are copied to all the ports as soon as you make them.

Table 90 Advanced Application > Multicast > Multicast Setting > MVR (continued)

LABEL	DESCRIPTION
Source Port	Select this option to set this port as the MVR source port that sends and receives multicast traffic. All source ports must belong to a single multicast VLAN.
Receiver Port	Select this option to set this port as a receiver port that only receives multicast traffic.
None	Select this option to set the port not to participate in MVR. No MVR multicast traffic is sent or received on this port.
Tagging	Select this checkbox if you want the port to tag the VLAN ID in all outgoing frames transmitted.
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
VLAN	This field displays the multicast VLAN ID. Click on an index number to change the settings.
Active	This field displays whether the multicast group is enabled or not.
Name	This field displays the descriptive name for this setting.
Mode	This field displays the MVR mode.
Source Port	This field displays the source port number(s).
Receiver Port	This field displays the receiver port number(s).
802.1p	This field displays the priority level.
Delete	To delete a multicast VLAN(s), select the rule(s) that you want to remove in the **Delete** column, then click the **Delete** button.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

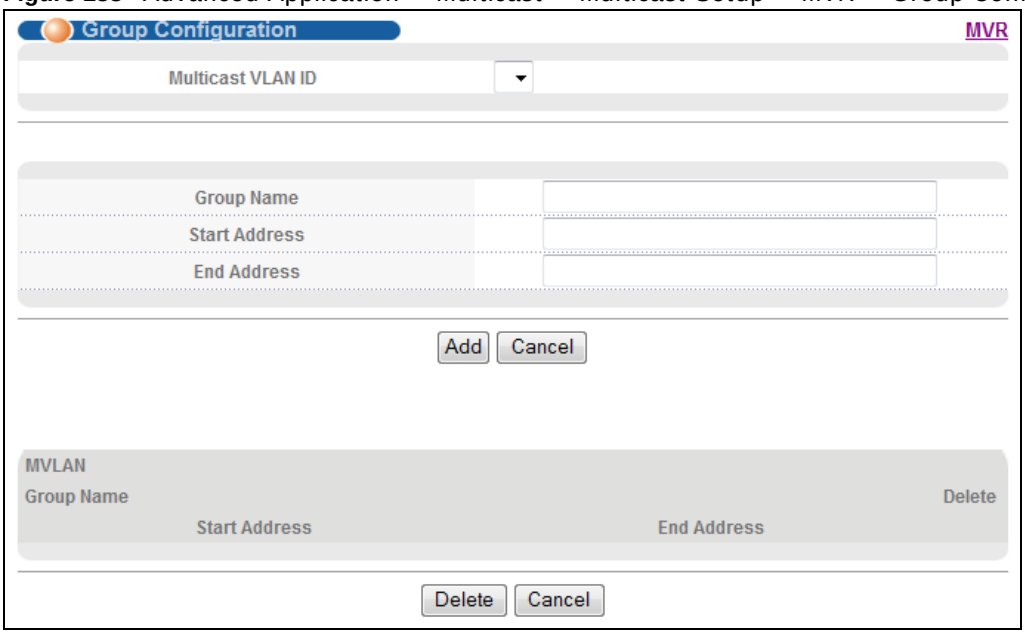
24.6.1 MVR Group Configuration

All source ports and receiver ports belonging to a multicast group can receive multicast data sent to this multicast group.

Use this screen to configure MVR IP multicast group address(es). Click the **Group Configuration** link in the **MVR** screen.

Note: A port can belong to more than one multicast VLAN. However, IP multicast group addresses in different multicast VLANs cannot overlap.

Figure 138 Advanced Application > Multicast > Multicast Setup > MVR > Group Configuration



The following table describes the labels in this screen.

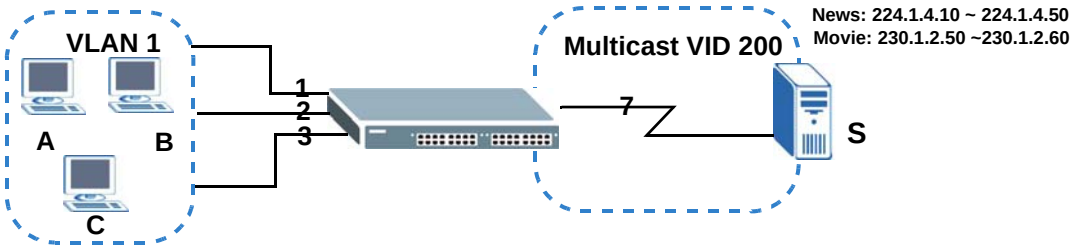
Table 91 Advanced Application > Multicast > Multicast Setting > MVR > Group Configuration

LABEL	DESCRIPTION
Multicast VLAN ID	Select a multicast VLAN ID (that you configured in the **MVR** screen) from the drop-down list box.
Group Name	Enter a descriptive name for identification purposes.
Start Address	Enter the starting IP multicast address of the multicast group in dotted decimal notation. Refer to Section on page 178 for more information on IP multicast addresses.
End Address	Enter the ending IP multicast address of the multicast group in dotted decimal notation. Enter the same IP address as the **Start Address** field if you want to configure only one IP address for a multicast group. Refer to Section on page 178 for more information on IP multicast addresses.
Add	Click this to create a new entry. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
MVLAN	This field displays the multicast VLAN ID.
Group Name	This field displays the descriptive name for this setting.
Start Address	This field displays the starting IP address of the multicast group.
End Address	This field displays the ending IP address of the multicast group.
Delete	Select the entry(ies) that you want to remove in the **Delete** column, then click the **Delete** button to remove the selected entry(ies) from the table. If you delete a multicast VLAN, all multicast groups in this VLAN will also be removed.
Cancel	Select **Cancel** to clear the checkbox(es) in the table.

24.6.2 MVR Configuration Example

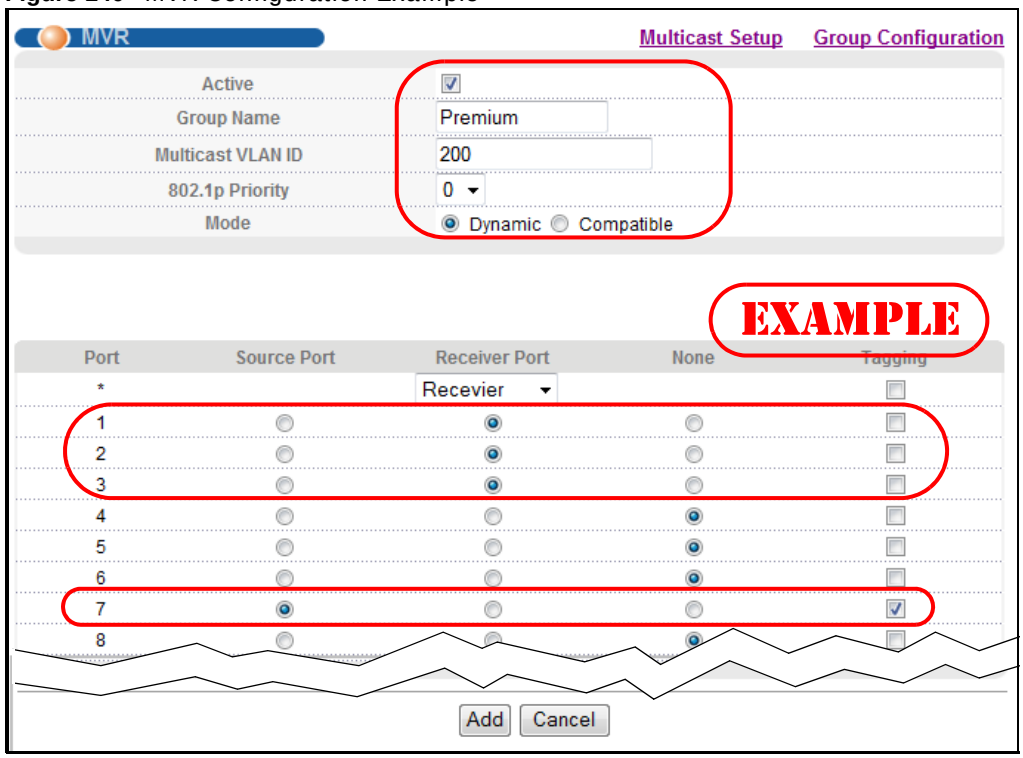
The following figure shows a network example where ports 1, 2 and 3 on the Switch belong to VLAN 1. In addition, port 7 belongs to the multicast group with VID 200 to receive multicast traffic (the **News** and **Movie** channels) from the remote streaming media server, **S**. Computers A, B and C in VLAN 1 are able to receive the traffic.

Figure 139 MVR Configuration Example



To configure the MVR settings on the Switch, create a multicast VLAN in the **MVR** screen and set the receiver and source ports.

Figure 140 MVR Configuration Example



To set the Switch to forward the multicast group traffic to the subscribers, configure multicast group settings in the **Group Configuration** screen. The following figure shows an example where two IPv4 multicast groups (**News** and **Movie**) are configured for the multicast VLAN 200.

Figure 141 MVR Group Configuration Example

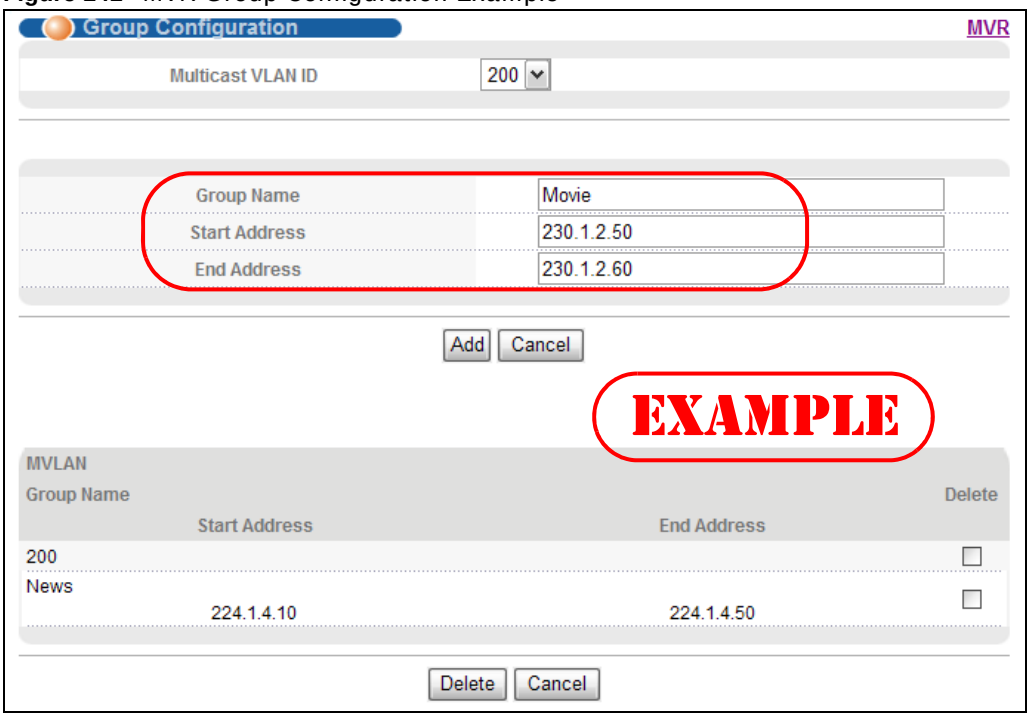
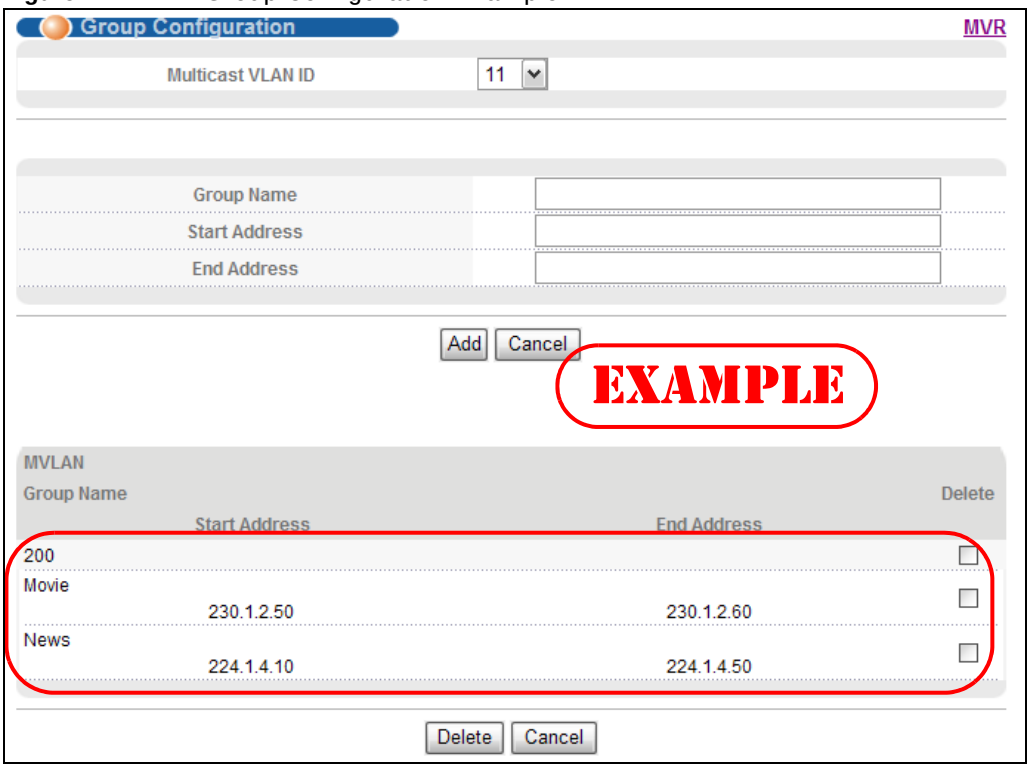


Figure 142 MVR Group Configuration Example



25

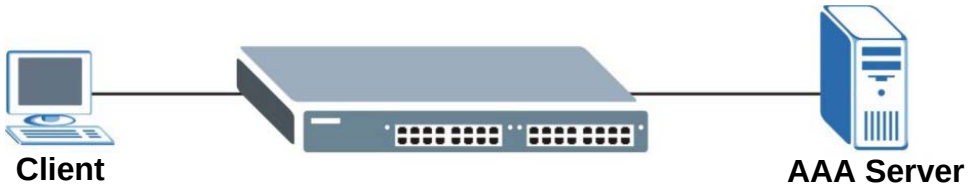
AAA

25.1 AAA Overview

This chapter describes how to configure authentication and authorization settings on the Switch.

The external servers that perform authentication and authorization functions are known as AAA servers. The Switch supports RADIUS (Remote Authentication Dial-In User Service, see Section on page 202) and TACACS+ (Terminal Access Controller Access-Control System Plus, see Section on page 202) as external authentication and authorization servers.

Figure 143 AAA Server



25.1.1 What You Can Do

- Use the **AAA** screen (Section 25.2 on page 202) to enable authentication and authorization or both of them on the Switch.
- use the **Radio Server Setup** screen (Section 25.3 on page 202) to configure your RADIUS server settings.
- Use the **TACACS+ Server Setup** screen (Section 25.4 on page 204) to configure your TACACS+ authentication settings.
- Use the **AAA Setup** screen (Section 25.5 on page 206) to specify the methods used to authenticate users accessing the Switch and specify which database the Switch should use first.

25.1.2 What You Need to Know

Authentication is the process of determining who a user is and validating access to the Switch. The Switch can authenticate users who try to log in based on user accounts configured on the Switch itself. The Switch can also use an external authentication server to authenticate a large number of users.

Authorization is the process of determining what a user is allowed to do. Different user accounts may have higher or lower privilege levels associated with them. For example, user A may have the right to create new login accounts on the Switch but user B cannot. The Switch can authorize users based on user accounts configured on the Switch itself or it can use an external server to authorize a large number of users.

Accounting is the process of recording what a user is doing. The Switch can use an external server to track when users log in, log out, execute commands and so on. Accounting can also record system related actions such as boot up and shut down times of the Switch.

Local User Accounts

By storing user profiles locally on the Switch, your Switch is able to authenticate and authorize users without interacting with a network AAA server. However, there is a limit on the number of users you may authenticate in this way (See Chapter 39 on page 318).

RADIUS and TACACS+

RADIUS and TACACS+ are security protocols used to authenticate users by means of an external server instead of (or in addition to) an internal device user database that is limited to the memory capacity of the device. In essence, RADIUS and TACACS+ authentication both allow you to validate an unlimited number of users from a central location.

The following table describes some key differences between RADIUS and TACACS+.

Table 92 RADIUS vs. TACACS+

	RADIUS	TACACS+
Transport Protocol	UDP (User Datagram Protocol)	TCP (Transmission Control Protocol)
Encryption	Encrypts the password sent for authentication.	All communication between the client (the Switch) and the TACACS server is encrypted.

25.2 AAA Screens

The **AAA** screens allow you to enable authentication and authorization or both of them on the Switch. First, configure your authentication server settings (RADIUS, TACACS+ or both) and then set up the authentication priority, activate authorization.

Click **Advanced Application** > **AAA** in the navigation panel to display the screen as shown.

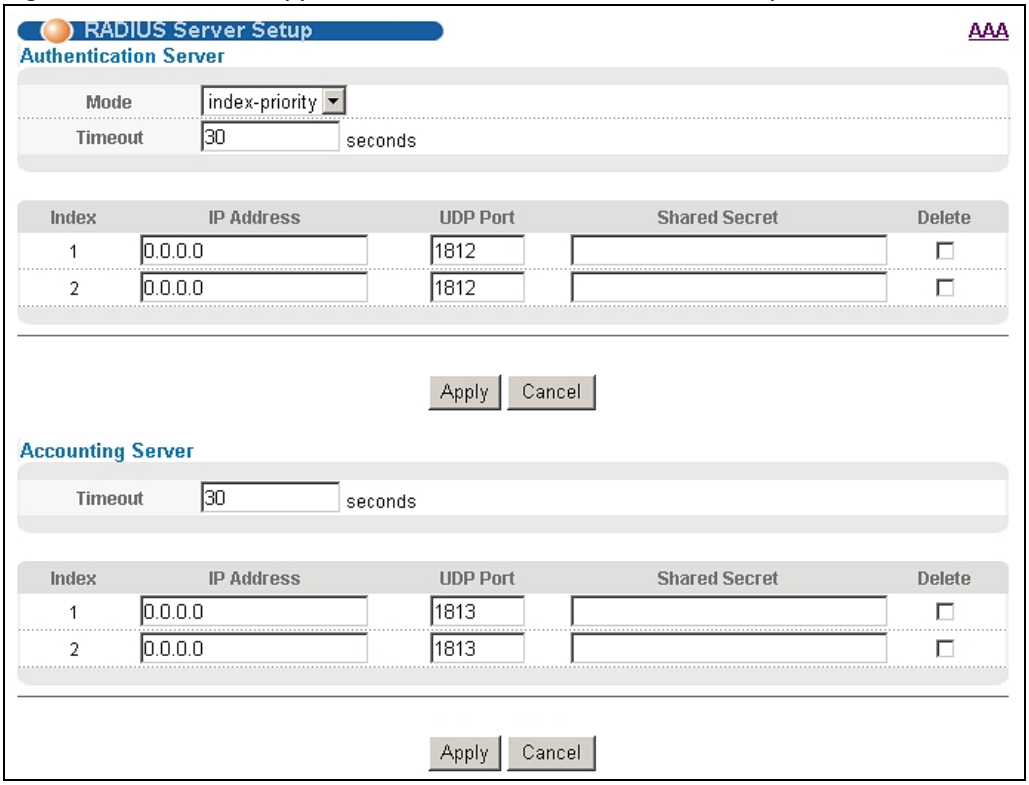
Figure 144 Advanced Application > AAA

25.3 RADIUS Server Setup

Use this screen to configure your RADIUS server settings. See Section on page 202 for more information on RADIUS servers and Section 25.6.2 on page 210 for RADIUS attributes utilized by

the authentication features on the Switch. Click on the **RADIUS Server Setup** link in the **AAA** screen to view the screen as shown.

Figure 145 Advanced Application > AAA > RADIUS Server Setup



The following table describes the labels in this screen.

Table 93 Advanced Application > AAA > RADIUS Server Setup

LABEL	DESCRIPTION
Authentication Server	Use this section to configure your RADIUS authentication settings.
Mode	This field is only valid if you configure multiple RADIUS servers. Select **index-priority** and the Switch tries to authenticate with the first configured RADIUS server, if the RADIUS server does not respond then the Switch tries to authenticate with the second RADIUS server. Select **round-robin** to alternate between the RADIUS servers that it sends authentication requests to.
Timeout	Specify the amount of time in seconds that the Switch waits for an authentication request response from the RADIUS server. If you are using **index-priority** for your authentication and you are using two RADIUS servers then the timeout value is divided between the two RADIUS servers. For example, if you set the timeout value to 30 seconds, then the Switch waits for a response from the first RADIUS server for 15 seconds and then tries the second RADIUS server.
Index	This is a read-only number representing a RADIUS server entry.
IP Address	Enter the IP address of an external RADIUS server in dotted decimal notation.
UDP Port	The default port of a RADIUS server for authentication is **1812**. You need not change this value unless your network administrator instructs you to do so.

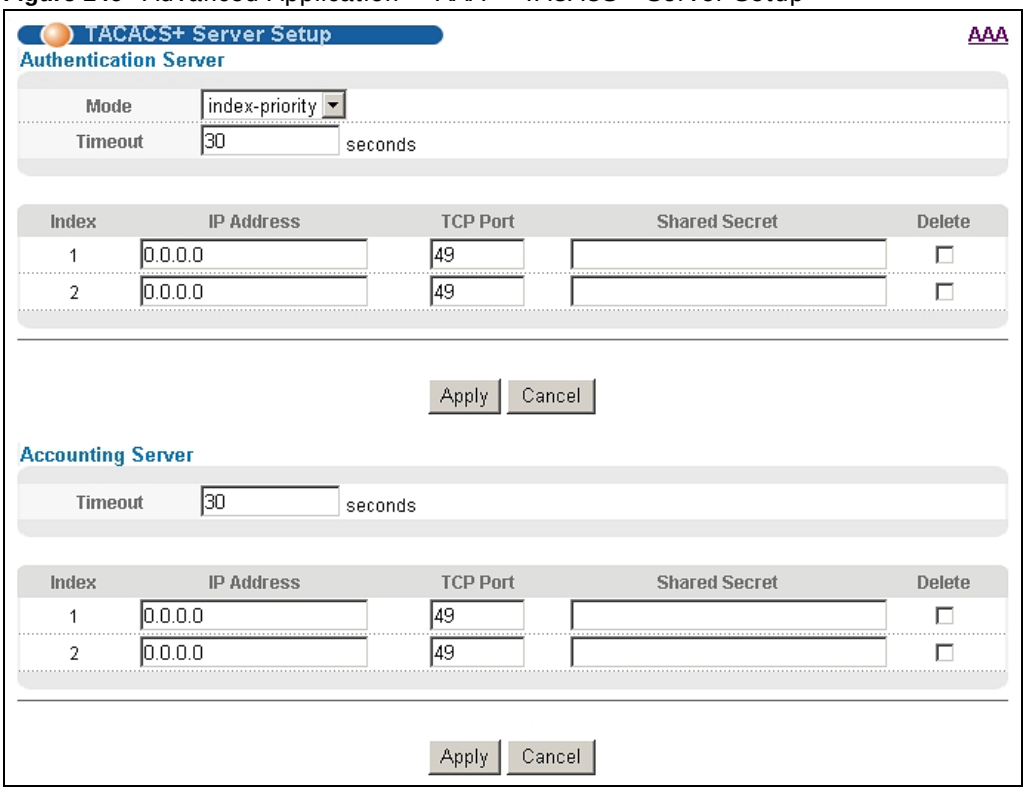
Table 93 Advanced Application > AAA > RADIUS Server Setup (continued)

LABEL	DESCRIPTION
Shared Secret	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external RADIUS server and the Switch. This key is not sent over the network. This key must be the same on the external RADIUS server and the Switch.
Delete	Check this box if you want to remove an existing RADIUS server entry from the Switch. This entry is deleted when you click **Apply**.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Accounting Server	Use this section to configure your RADIUS accounting server settings.
Timeout	Specify the amount of time in seconds that the Switch waits for an accounting request response from the RADIUS accounting server.
Index	This is a read-only number representing a RADIUS accounting server entry.
IP Address	Enter the IP address of an external RADIUS accounting server in dotted decimal notation.
UDP Port	The default port of a RADIUS accounting server for accounting is **1813**. You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external RADIUS accounting server and the Switch. This key is not sent over the network. This key must be the same on the external RADIUS accounting server and the Switch.
Delete	Check this box if you want to remove an existing RADIUS accounting server entry from the Switch. This entry is deleted when you click **Apply**.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

25.4 TACACS+ Server Setup

Use this screen to configure your TACACS+ server settings. See Section on page 202 for more information on TACACS+ servers. Click on the **TACACS+ Server Setup** link in the **AAA** screen to view the screen as shown.

Figure 146 Advanced Application > AAA > TACACS+ Server Setup



The following table describes the labels in this screen.

Table 94 Advanced Application > AAA > TACACS+ Server Setup

LABEL	DESCRIPTION
Authentication Server	Use this section to configure your TACACS+ authentication settings.
Mode	This field is only valid if you configure multiple TACACS+ servers. Select **index-priority** and the Switch tries to authenticate with the first configured TACACS+ server, if the TACACS+ server does not respond then the Switch tries to authenticate with the second TACACS+ server. Select **round-robin** to alternate between the TACACS+ servers that it sends authentication requests to.
Timeout	Specify the amount of time in seconds that the Switch waits for an authentication request response from the TACACS+ server. If you are using **index-priority** for your authentication and you are using two TACACS+ servers then the timeout value is divided between the two TACACS+ servers. For example, if you set the timeout value to 30 seconds, then the Switch waits for a response from the first TACACS+ server for 15 seconds and then tries the second TACACS+ server.
Index	This is a read-only number representing a TACACS+ server entry.
IP Address	Enter the IP address of an external TACACS+ server in dotted decimal notation.
TCP Port	The default port of a TACACS+ server for authentication is **49**. You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external TACACS+ server and the Switch. This key is not sent over the network. This key must be the same on the external TACACS+ server and the Switch.

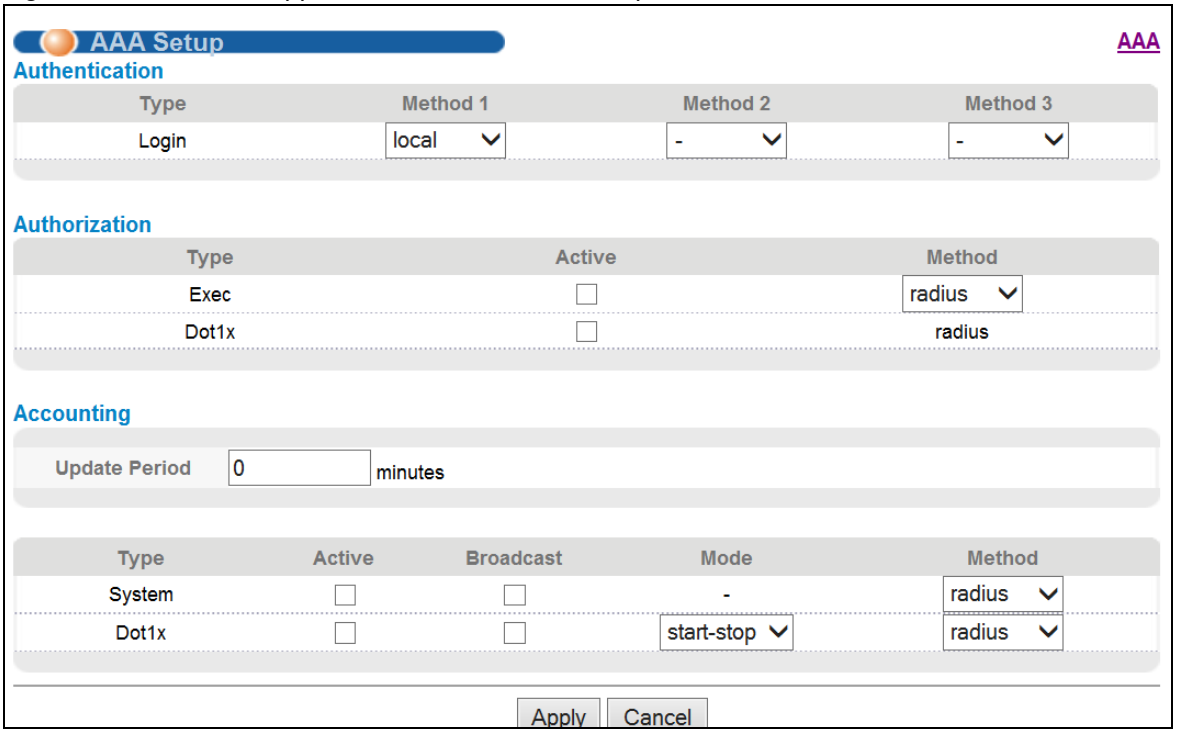
Table 94 Advanced Application > AAA > TACACS+ Server Setup (continued)

LABEL	DESCRIPTION
Delete	Check this box if you want to remove an existing TACACS+ server entry from the Switch. This entry is deleted when you click **Apply**.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Accounting Server	Use this section to configure your TACACS+ accounting settings.
Timeout	Specify the amount of time in seconds that the Switch waits for an accounting request response from the TACACS+ server.
Index	This is a read-only number representing a TACACS+ accounting server entry.
IP Address	Enter the IP address of an external TACACS+ accounting server in dotted decimal notation.
TCP Port	The default port of a TACACS+ accounting server is **49**. You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external TACACS+ accounting server and the Switch. This key is not sent over the network. This key must be the same on the external TACACS+ accounting server and the Switch.
Delete	Check this box if you want to remove an existing TACACS+ accounting server entry from the Switch. This entry is deleted when you click **Apply**.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

25.5 AAA Setup

Use this screen to configure authentication and authorization settings on the Switch. Click on the **AAA Setup** link in the **AAA** screen to view the screen as shown.

Figure 147 Advanced Application > AAA > AAA Setup



The following table describes the labels in this screen.

Table 95 Advanced Application > AAA > AAA Setup

LABEL	DESCRIPTION
Authentication	Use this section to specify the methods used to authenticate users accessing the Switch.
Login	These fields specify which database the Switch should use (first, second and third) to authenticate administrator accounts (users for Switch management). Configure the local user accounts in the **Access Control > Logins** screen. The TACACS+ and RADIUS are external servers. Before you specify the priority, make sure you have set up the corresponding database correctly first. You can specify up to three methods for the Switch to authenticate administrator accounts. The Switch checks the methods in the order you configure them (first **Method 1**, then **Method 2** and finally **Method 3**). You must configure the settings in the **Method 1** field. If you want the Switch to check other sources for administrator accounts, specify them in **Method 2** and **Method 3** fields. Select **local** to have the Switch check the administrator accounts configured in the **Access Control > Logins** screen. Select **radius** to have the Switch check the administrator accounts configured via your RADIUS server. Select **tacacs+** to have the Switch check the administrator accounts configured via your TACACS+ server.
Authorization	Use this section to configure authorization settings on the Switch.
Type	Set whether the Switch provides the following services to a user. • **Exec**: Allow an administrator who logs into the Switch to have a different access privilege level assigned via the external server. • **Dot1x**: Allow an IEEE 802.1x client to have different bandwidth limit or VLAN ID assigned via the external server.
Active	Select this to activate authorization for a specified event types.

Table 95 Advanced Application > AAA > AAA Setup (continued)

LABEL	DESCRIPTION
Method	Select whether you want to use RADIUS or TACACS+ for authorization of specific types of events. RADIUS is the only method for IEEE 802.1x authorization.
Accounting	Use this section to configure accounting settings on the Switch.
Update Period	This is the amount of time in minutes before the Switch sends an update to the accounting server. This is only valid if you select the **start-stop** option for the **Dot1x** entry.
Type	The Switch supports the following types of events to be sent to the accounting server(s): • **System** - Configure the Switch to send information when the following system events occur: system boots up, system shuts down, system accounting is enabled, system accounting is disabled • **Dot1x** - Configure the Switch to send information when an IEEE 802.1x client begins a session (authenticates via the Switch), ends a session as well as interim updates of a session.
Active	Select this to activate accounting for a specified event types.
Broadcast	Select this to have the Switch send accounting information to all configured accounting servers at the same time. If you don't select this and you have two accounting servers set up, then the Switch sends information to the first accounting server and if it doesn't get a response from the accounting server then it tries the second accounting server.
Mode	The Switch supports two modes of recording login events. Select: • **start-stop** - to have the Switch send information to the accounting server when a user begins a session, during a user's session (if it lasts past the **Update Period**), and when a user ends a session. • **stop-only** - to have the Switch send information to the accounting server only when a user ends a session.
Method	Select whether you want to use RADIUS or TACACS+ for accounting of specific types of events. RADIUS is the only method for IEEE 802.1x authorization.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

25.6 Technical Reference

This section provides technical background information on the topics discussed in this chapter.

25.6.1 Vendor Specific Attribute

RFC 2865 standard specifies a method for sending vendor-specific information between a RADIUS server and a network access device (for example, the Switch). A company can create Vendor Specific Attributes (VSAs) to expand the functionality of a RADIUS server.

The Switch supports VSAs that allow you to perform the following actions based on user authentication:

- Limit bandwidth on incoming or outgoing traffic for the port the user connects to.
- Assign account privilege levels for the authenticated user.

The VSAs are composed of the following:

- **Vendor-ID**: An identification number assigned to the company by the IANA (Internet Assigned Numbers Authority). ZyXEL's vendor ID is 890.
- **Vendor-Type**: A vendor specified attribute, identifying the setting you want to modify.
- **Vendor-data**: A value you want to assign to the setting.

Note: Refer to the documentation that comes with your RADIUS server on how to configure VSAs for users authenticating via the RADIUS server.

The following table describes the VSAs supported on the Switch.

Table 96 Supported VSAs

FUNCTION	ATTRIBUTE
Ingress Bandwidth Assignment	Vendor-Id = **890** Vendor-Type = **1** Vendor-data = ingress rate (Kbps in decimal format)
Egress Bandwidth Assignment	Vendor-Id = **890** Vendor-Type = **2** Vendor-data = egress rate (Kbps in decimal format)
Privilege Assignment	Vendor-ID = **890** Vendor-Type = **3** Vendor-Data = "**shell:priv-lvl=**N" or Vendor-ID = **9** (CISCO) Vendor-Type = **1** (CISCO-AVPAIR) Vendor-Data = "**shell:priv-lvl=**N" where N is a privilege level (from 0 to 14). Note: If you set the privilege level of a login account differently on the RADIUS server(s) and the Switch, the user is assigned a privilege level from the database (RADIUS or local) the Switch uses first for user authentication.

25.6.1.1 Tunnel Protocol Attribute

You can configure tunnel protocol attributes on the RADIUS server (refer to your RADIUS server documentation) to assign a port on the Switch to a VLAN based on IEEE 802.1x authentication. The port VLAN settings are fixed and untagged. This will also set the port's VID. The following table

describes the values you need to configure. Note that the bolded values in the table are fixed values as defined in RFC 3580.

Table 97 Supported Tunnel Protocol Attribute

FUNCTION	ATTRIBUTE
VLAN Assignment	Tunnel-Type = **VLAN(13)** Tunnel-Medium-Type = **802(6)** Tunnel-Private-Group-ID = VLAN ID Note: You must also create a VLAN with the specified VID on the Switch.

25.6.2 Supported RADIUS Attributes

Remote Authentication Dial-In User Service (RADIUS) attributes are data used to define specific authentication elements in a user profile, which is stored on the RADIUS server. This appendix lists the RADIUS attributes supported by the Switch.

Refer to RFC 2865 for more information about RADIUS attributes used for authentication.

This section lists the attributes used by authentication functions on the Switch. In cases where the attribute has a specific format associated with it, the format is specified.

25.6.3 Attributes Used for Authentication

The following sections list the attributes sent from the Switch to the RADIUS server when performing authentication.

25.6.3.1 Attributes Used for Authenticating Privilege Access

User-Name

- The format of the User-Name attribute is **$enab#$**, where # is the privilege level (1-14).

User-Password

NAS-Identifier

NAS-IP-Address

25.6.3.2 Attributes Used to Login Users

User-Name

User-Password

NAS-Identifier

NAS-IP-Address

25.6.3.3 Attributes Used by the IEEE 802.1x Authentication

User-Name

NAS-Identifier

NAS-IP-Address

NAS-Port

NAS-Port-Type

- This value is set to **Ethernet(15)** on the Switch.

Calling-Station-Id

Frame-MTU

EAP-Message

State

Message-Authenticator

26

IP Source Guard

26.1 Overview

Use IP source guard to filter unauthorized DHCP and ARP packets in your network.

IP source guard uses a binding table to distinguish between authorized and unauthorized DHCP and ARP packets in your network. A binding contains these key attributes:

- MAC address
- VLAN ID
- IP address
- Port number

When the Switch receives a DHCP or ARP packet, it looks up the appropriate MAC address, VLAN ID, IP address, and port number in the binding table. If there is a binding, the Switch forwards the packet. If there is not a binding, the Switch discards the packet.

26.1.1 What You Can Do

- Use the **IP Source Guard** screen (Section 26.2 on page 213) to look at the current bindings for DHCP snooping and ARP inspection.
- Use the **IP Source Guard Static Binding** screen (Section 26.3 on page 214) to manage static bindings for DHCP snooping and ARP inspection.
- Use the **DHCP Snooping** screen (Section 26.4 on page 215) to look at various statistics about the DHCP snooping database.
- Use this **DHCP Snooping Configure** screen (Section 26.5 on page 218) to enable DHCP snooping on the Switch (not on specific VLAN), specify the VLAN where the default DHCP server is located, and configure the DHCP snooping database.
- Use the **DHCP Snooping Port Configure** screen (Section 26.5.1 on page 220) to specify whether ports are trusted or untrusted ports for DHCP snooping.
- Use the **DHCP VLAN Configure** screen (Section 26.5.2 on page 221) to enable DHCP snooping on each VLAN and to specify whether or not the Switch adds DHCP relay agent option 82 information to DHCP requests that the Switch relays to a DHCP server for each VLAN.
- Use the **DHCP Snooping VLAN Port Configure** screen (Section 26.5.3 on page 222) to apply a different DHCP option 82 profile to certain ports in a VLAN.
- Use the **ARP Inspection Status** screen (Section 26.6 on page 223) to look at the current list of MAC address filters that were created because the Switch identified an unauthorized ARP packet.
- Use the **ARP Inspection VLAN Status** screen (Section 26.7 on page 224) to look at various statistics about ARP packets in each VLAN.
- Use the **ARP Inspection Log Status** screen (Section 26.8 on page 225) to look at log messages that were generated by ARP packets and that have not been sent to the syslog server yet.

- Use the **ARP Inspection Configure** screen (Section 26.9 on page 227) to enable ARP inspection on the Switch. You can also configure the length of time the Switch stores records of discarded ARP packets and global settings for the ARP inspection log.
- Use the **ARP Inspection Port Configure** screen (Section 26.9.1 on page 228) to specify whether ports are trusted or untrusted ports for ARP inspection.
- Use the **ARP Inspection VLAN Configure** screen (Section 26.9.2 on page 230) to enable ARP inspection on each VLAN and to specify when the Switch generates log messages for receiving ARP packets from each VLAN.

26.1.2 What You Need to Know

The Switch builds the binding table by snooping DHCP packets (dynamic bindings) and from information provided manually by administrators (static bindings).

IP source guard consists of the following features:

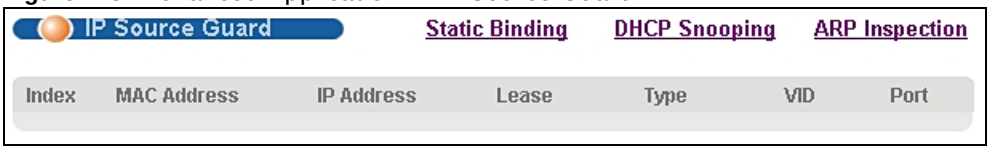
- Static bindings. Use this to create static bindings in the binding table.
- DHCP snooping. Use this to filter unauthorized DHCP packets on the network and to build the binding table dynamically.
- ARP inspection. Use this to filter unauthorized ARP packets on the network.

If you want to use dynamic bindings to filter unauthorized ARP packets (typical implementation), you have to enable DHCP snooping before you enable ARP inspection.

26.2 IP Source Guard

Use this screen to look at the current bindings for DHCP snooping and ARP inspection. Bindings are used by DHCP snooping and ARP inspection to distinguish between authorized and unauthorized packets in the network. The Switch learns the bindings by snooping DHCP packets (dynamic bindings) and from information provided manually by administrators (static bindings). To open this screen, click **Advanced Application > IP Source Guard**.

Figure 148 Advanced Application > IP Source Guard



The following table describes the labels in this screen.

Table 98 Advanced Application > IP Source Guard

LABEL	DESCRIPTION
Index	This field displays a sequential number for each binding.
MAC Address	This field displays the source MAC address in the binding.
IP Address	This field displays the IP address assigned to the MAC address in the binding.
Lease	This field displays how many days, hours, minutes, and seconds the binding is valid; for example, **2d3h4m5s** means the binding is still valid for 2 days, 3 hours, 4 minutes, and 5 seconds. This field displays **infinity** if the binding is always valid (for example, a static binding).

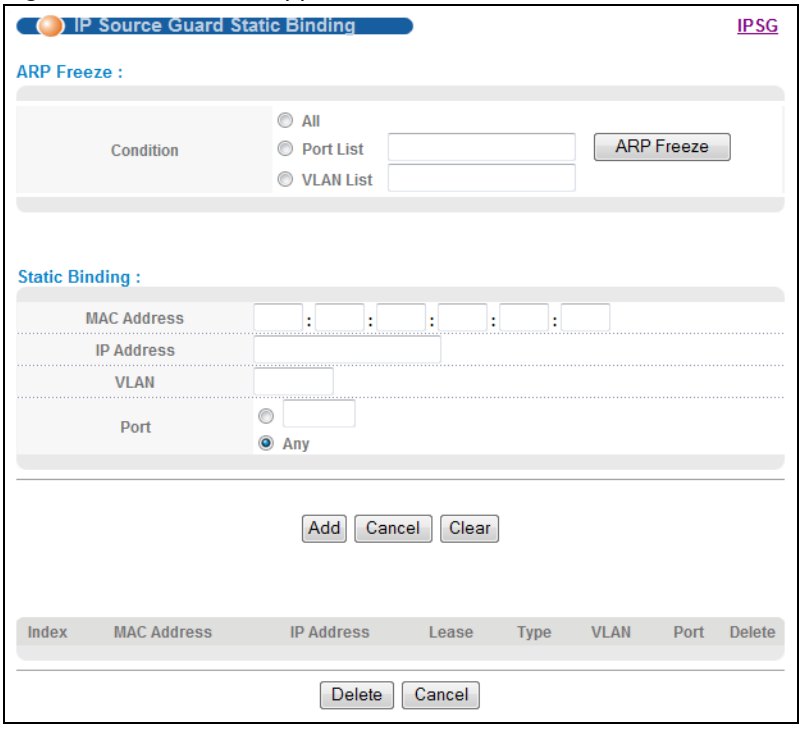
Table 98 Advanced Application > IP Source Guard (continued)

LABEL	DESCRIPTION
Type	This field displays how the Switch learned the binding. **static**: This binding was learned from information provided manually by an administrator. **dhcp-snooping**: This binding was learned by snooping DHCP packets.
VID	This field displays the source VLAN ID in the binding.
Port	This field displays the port number in the binding. If this field is blank, the binding applies to all ports.

26.3 IP Source Guard Static Binding

Use this screen to manage static bindings for DHCP snooping and ARP inspection. Static bindings are uniquely identified by the MAC address and VLAN ID. Each MAC address and VLAN ID can only be in one static binding. If you try to create a static binding with the same MAC address and VLAN ID as an existing static binding, the new static binding replaces the original one. To open this screen, click **Advanced Application > IP Source Guard > Static Binding**.

Figure 149 Advanced Application > IP Source Guard > Static Binding



The following table describes the labels in this screen.

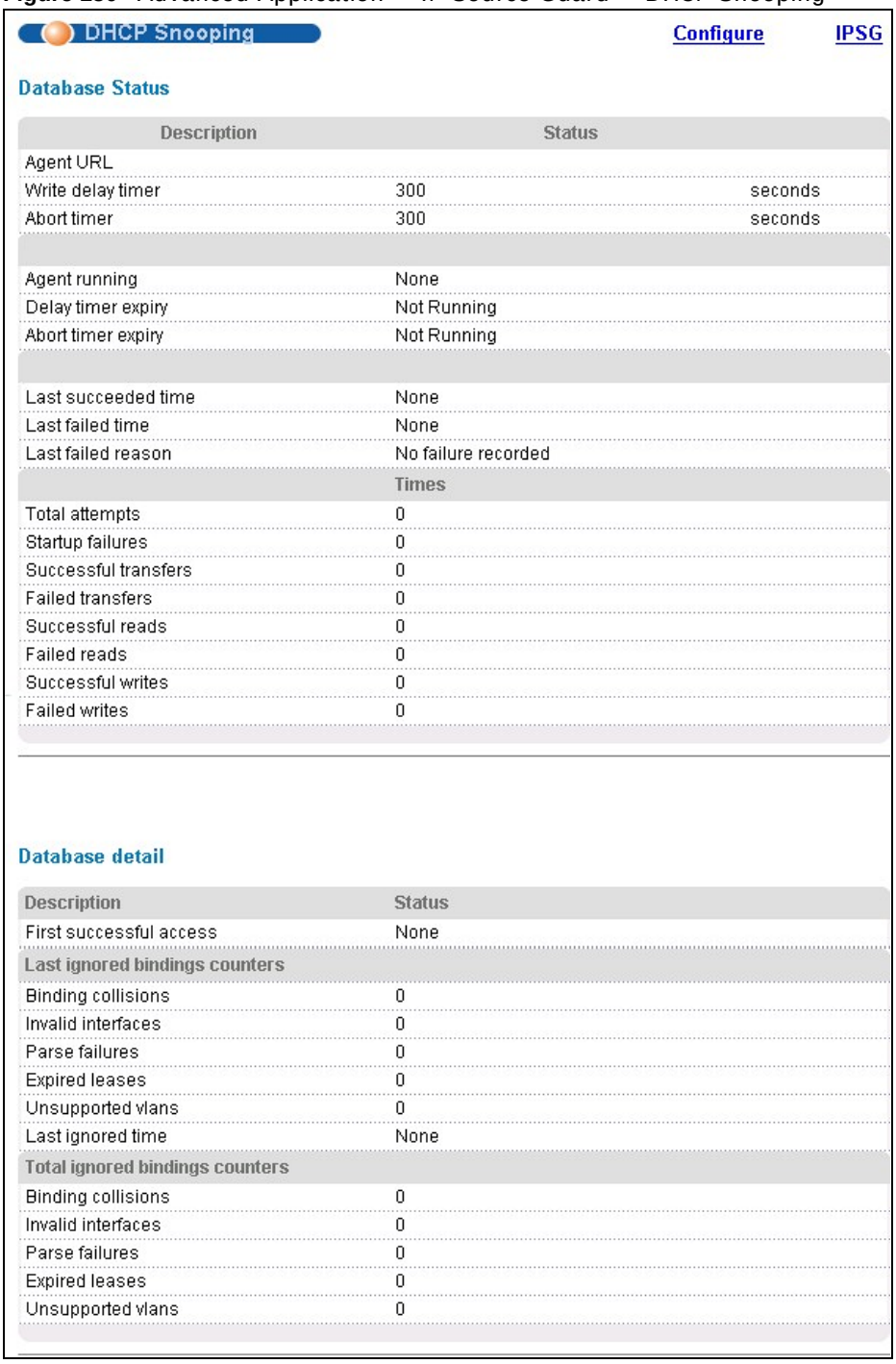
Table 99 Advanced Application > IP Source Guard > Static Binding

LABEL	DESCRIPTION
ARP Freeze	ARP Freeze allows you to automatically create static bindings from the current ARP entries (either dynamically learned or static ARP entries) until the Switch's binding table is full. Note: The ARP learning mode should be set to **ARP-Request** in the **IP Application > ARP Setup > ARP Learning** screen before you use the ARP Freeze feature.
Condition	**All** - Select this and click **ARP Freeze** to have the Switch automatically add all the current ARP entries to the static bindings table. **Port List** - Select this and enter the number of the port(s) (separated by a comma). ARP entries learned on the specified port(s) are added to the static bindings table after you click **ARP Freeze**. **VLAN List** - Select this and enter the ID number of the VLAN(s) (separated by a comma). ARP entries for the specified VLAN(s) are added to the static bindings table after you click **ARP Freeze**.
Static Binding	
MAC Address	Enter the source MAC address in the binding.
IP Address	Enter the IP address assigned to the MAC address in the binding.
VLAN	Enter the source VLAN ID in the binding.
Port	Specify the port(s) in the binding. If this binding has one port, select the first radio button and enter the port number in the field to the right. If this binding applies to all ports, select **Any**.
Add	Click this to create the specified static binding or to update an existing one.
Cancel	Click this to reset the values above based on the last selected static binding or, if not applicable, to clear the fields above.
Clear	Click this to clear the fields above.
Index	This field displays a sequential number for each binding.
MAC Address	This field displays the source MAC address in the binding.
IP Address	This field displays the IP address assigned to the MAC address in the binding.
Lease	This field displays how long the binding is valid.
Type	This field displays how the Switch learned the binding. **static**: This binding was learned from information provided manually by an administrator.
VLAN	This field displays the source VLAN ID in the binding.
Port	This field displays the port number in the binding. If this field is blank, the binding applies to all ports.
Delete	Select this, and click **Delete** to remove the specified entry.
Cancel	Click this to clear the **Delete** check boxes above.

26.4 DHCP Snooping

Use this screen to look at various statistics about the DHCP snooping database. To open this screen, click **Advanced Application > IP Source Guard > DHCP Snooping**.

Figure 150 Advanced Application > IP Source Guard > DHCP Snooping



The following table describes the labels in this screen.

Table 100 Advanced Application > IP Source Guard > DHCP Snooping

LABEL	DESCRIPTION
Database Status	This section displays the current settings for the DHCP snooping database. You can configure them in the **DHCP Snooping Configure** screen. See Section 26.5 on page 218.
Agent URL	This field displays the location of the DHCP snooping database.

Table 100 Advanced Application > IP Source Guard > DHCP Snooping (continued)

LABEL	DESCRIPTION
Write delay timer	This field displays how long (in seconds) the Switch tries to complete a specific update in the DHCP snooping database before it gives up.
Abort timer	This field displays how long (in seconds) the Switch waits to update the DHCP snooping database after the current bindings change.
	This section displays information about the current update and the next update of the DHCP snooping database.
Agent running	This field displays the status of the current update or access of the DHCP snooping database. **none**: The Switch is not accessing the DHCP snooping database. **read**: The Switch is loading dynamic bindings from the DHCP snooping database. **write**: The Switch is updating the DHCP snooping database.
Delay timer expiry	This field displays how much longer (in seconds) the Switch tries to complete the current update before it gives up. It displays **Not Running** if the Switch is not updating the DHCP snooping database right now.
Abort timer expiry	This field displays when (in seconds) the Switch is going to update the DHCP snooping database again. It displays **Not Running** if the current bindings have not changed since the last update.
	This section displays information about the last time the Switch updated the DHCP snooping database.
Last succeeded time	This field displays the last time the Switch updated the DHCP snooping database successfully.
Last failed time	This field displays the last time the Switch updated the DHCP snooping database unsuccessfully.
Last failed reason	This field displays the reason the Switch updated the DHCP snooping database unsuccessfully.
	This section displays historical information about the number of times the Switch successfully or unsuccessfully read or updated the DHCP snooping database.
Total attempts	This field displays the number of times the Switch has tried to access the DHCP snooping database for any reason.
Startup failures	This field displays the number of times the Switch could not create or read the DHCP snooping database when the Switch started up or a new URL is configured for the DHCP snooping database.
Successful transfers	This field displays the number of times the Switch read bindings from or updated the bindings in the DHCP snooping database successfully.
Failed transfers	This field displays the number of times the Switch was unable to read bindings from or update the bindings in the DHCP snooping database.
Successful reads	This field displays the number of times the Switch read bindings from the DHCP snooping database successfully.
Failed reads	This field displays the number of times the Switch was unable to read bindings from the DHCP snooping database.
Successful writes	This field displays the number of times the Switch updated the bindings in the DHCP snooping database successfully.
Failed writes	This field displays the number of times the Switch was unable to update the bindings in the DHCP snooping database.
Database detail	
First successful access	This field displays the first time the Switch accessed the DHCP snooping database for any reason.

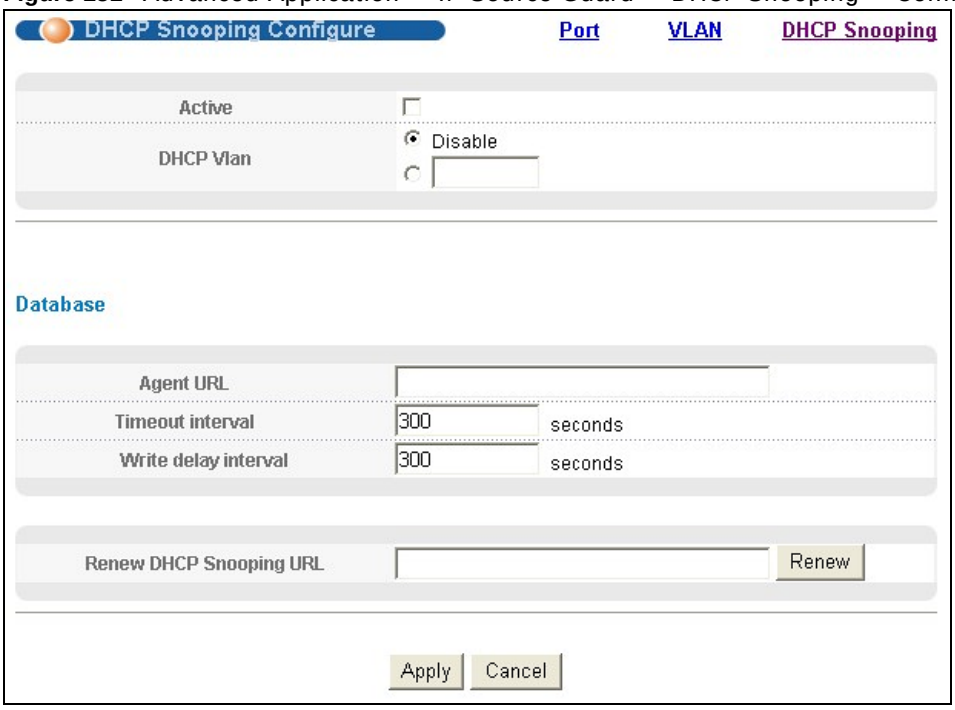
Table 100 Advanced Application > IP Source Guard > DHCP Snooping (continued)

LABEL	DESCRIPTION
Last ignored bindings counters	This section displays the number of times and the reasons the Switch ignored bindings the last time it read bindings from the DHCP binding database. You can clear these counters by restarting the Switch.
Binding collisions	This field displays the number of bindings the Switch ignored because the Switch already had a binding with the same MAC address and VLAN ID.
Invalid interfaces	This field displays the number of bindings the Switch ignored because the port number was a trusted interface or does not exist anymore.
Parse failures	This field displays the number of bindings the Switch ignored because the Switch was unable to understand the binding in the DHCP binding database.
Expired leases	This field displays the number of bindings the Switch ignored because the lease time had already expired.
Unsupported vlans	This field displays the number of bindings the Switch ignored because the VLAN ID does not exist anymore.
Last ignored time	This field displays the last time the Switch ignored any bindings for any reason from the DHCP binding database.
Total ignored bindings counters	This section displays the reasons the Switch has ignored bindings any time it read bindings from the DHCP binding database. You can clear these counters by restarting the Switch.
Binding collisions	This field displays the number of bindings the Switch has ignored because the Switch already had a binding with the same MAC address and VLAN ID.
Invalid interfaces	This field displays the number of bindings the Switch has ignored because the port number was a trusted interface or does not exist anymore.
Parse failures	This field displays the number of bindings the Switch has ignored because the Switch was unable to understand the binding in the DHCP binding database.
Expired leases	This field displays the number of bindings the Switch has ignored because the lease time had already expired.
Unsupported vlans	This field displays the number of bindings the Switch has ignored because the VLAN ID does not exist anymore.

26.5 DHCP Snooping Configure

Use this screen to enable DHCP snooping on the Switch (not on specific VLAN), specify the VLAN where the default DHCP server is located, and configure the DHCP snooping database. The DHCP snooping database stores the current bindings on a secure, external TFTP server so that they are still available after a restart. To open this screen, click **Advanced Application > IP Source Guard > DHCP Snooping > Configure**.

Figure 151 Advanced Application > IP Source Guard > DHCP Snooping > Configure



The following table describes the labels in this screen.

Table 101 Advanced Application > IP Source Guard > DHCP Snooping > Configure

LABEL	DESCRIPTION
Active	Select this to enable DHCP snooping on the Switch. You still have to enable DHCP snooping on specific VLAN and specify trusted ports. Note: If DHCP is enabled and there are no trusted ports, DHCP requests will not succeed.
DHCP Vlan	Select a VLAN ID if you want the Switch to forward DHCP packets to DHCP servers on a specific VLAN. Note: You have to enable DHCP snooping on the DHCP VLAN too. You can enable **Option82** in the **DHCP Snooping VLAN Configure** screen (Section 26.5.2 on page 221) to help the DHCP servers distinguish between DHCP requests from different VLAN. Select **Disable** if you do not want the Switch to forward DHCP packets to a specific VLAN.
Database	If **Timeout interval** is greater than **Write delay interval**, it is possible that the next update is scheduled to occur before the current update has finished successfully or timed out. In this case, the Switch waits to start the next update until it completes the current one.
Agent URL	Enter the location of the DHCP snooping database. The location should be expressed like this: **tftp://{domain name or IP address}/directory, if applicable/file name**; for example, **tftp://192.168.10.1/database.txt**.
Timeout interval	Enter how long (10-65535 seconds) the Switch tries to complete a specific update in the DHCP snooping database before it gives up.

Table 101 Advanced Application > IP Source Guard > DHCP Snooping > Configure (continued)

LABEL	DESCRIPTION
Write delay interval	Enter how long (10-65535 seconds) the Switch waits to update the DHCP snooping database the first time the current bindings change after an update. Once the next update is scheduled, additional changes in current bindings are automatically included in the next update.
Renew DHCP Snooping URL	Enter the location of a DHCP snooping database, and click **Renew** if you want the Switch to load it. You can use this to load dynamic bindings from a different DHCP snooping database than the one specified in **Agent URL**. When the Switch loads dynamic bindings from a DHCP snooping database, it does not discard the current dynamic bindings first. If there is a conflict, the Switch keeps the dynamic binding in volatile memory and updates the **Binding collisions** counter in the **DHCP Snooping** screen (Section 26.4 on page 215).
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values in this screen to their last-saved values.

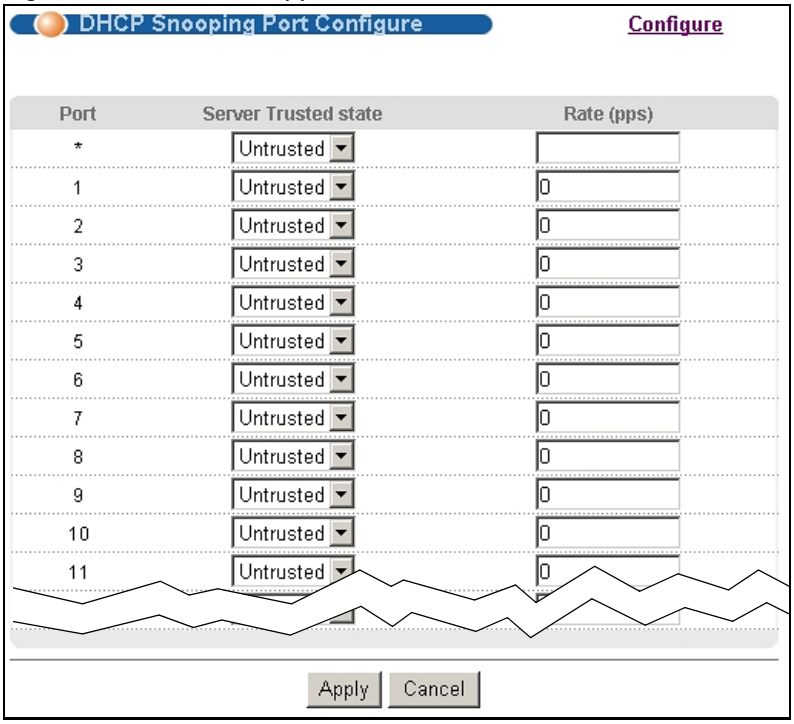
26.5.1 DHCP Snooping Port Configure

Use this screen to specify whether ports are trusted or untrusted ports for DHCP snooping.

Note: If DHCP snooping is enabled but there are no trusted ports, DHCP requests cannot reach the DHCP server.

You can also specify the maximum number for DHCP packets that each port (trusted or untrusted) can receive each second. To open this screen, click **Advanced Application > IP Source Guard > DHCP Snooping > Configure > Port**.

Figure 152 Advanced Application > IP Source Guard > DHCP Snooping > Configure > Port



The following table describes the labels in this screen.

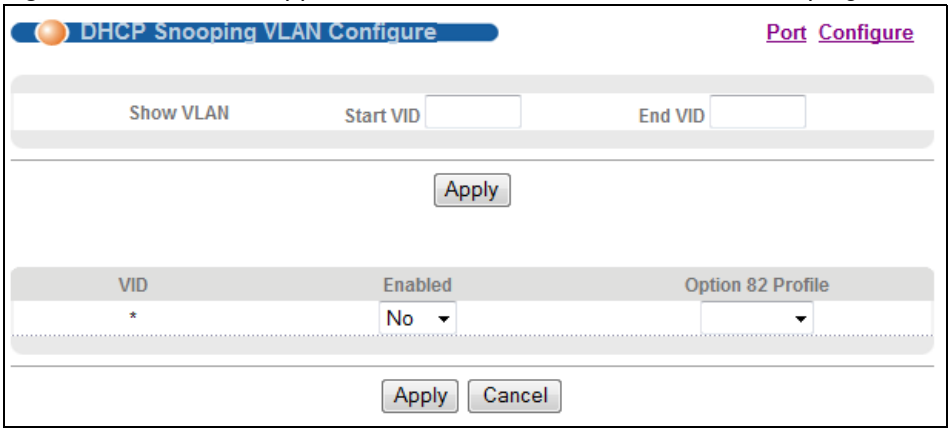
Table 102 Advanced Application > IP Source Guard > DHCP Snooping > Configure > Port

LABEL	DESCRIPTION
Port	This field displays the port number. If you configure the * port, the settings are applied to all of the ports.
Server Trusted state	Select whether this port is a trusted port (**Trusted**) or an untrusted port (**Untrusted**). Trusted ports are connected to DHCP servers or other switches, and the Switch discards DHCP packets from trusted ports only if the rate at which DHCP packets arrive is too high. Untrusted ports are connected to subscribers, and the Switch discards DHCP packets from untrusted ports in the following situations: • The packet is a DHCP server packet (for example, OFFER, ACK, or NACK). • The source MAC address and source IP address in the packet do not match any of the current bindings. • The packet is a RELEASE or DECLINE packet, and the source MAC address and source port do not match any of the current bindings. • The rate at which DHCP packets arrive is too high.
Rate (pps)	Specify the maximum number for DHCP packets (1-2048) that the Switch receives from each port each second. The Switch discards any additional DHCP packets. Enter 0 to disable this limit, which is recommended for trusted ports.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values in this screen to their last-saved values.

26.5.2 DHCP Snooping VLAN Configure

Use this screen to enable DHCP snooping on each VLAN and to specify whether or not the Switch adds DHCP relay agent option 82 information (Chapter 37 on page 300) to DHCP requests that the Switch relays to a DHCP server for each VLAN. To open this screen, click **Advanced Application > IP Source Guard > DHCP Snooping > Configure > VLAN**.

Figure 153 Advanced Application > IP Source Guard > DHCP Snooping > Configure > VLAN



The following table describes the labels in this screen.

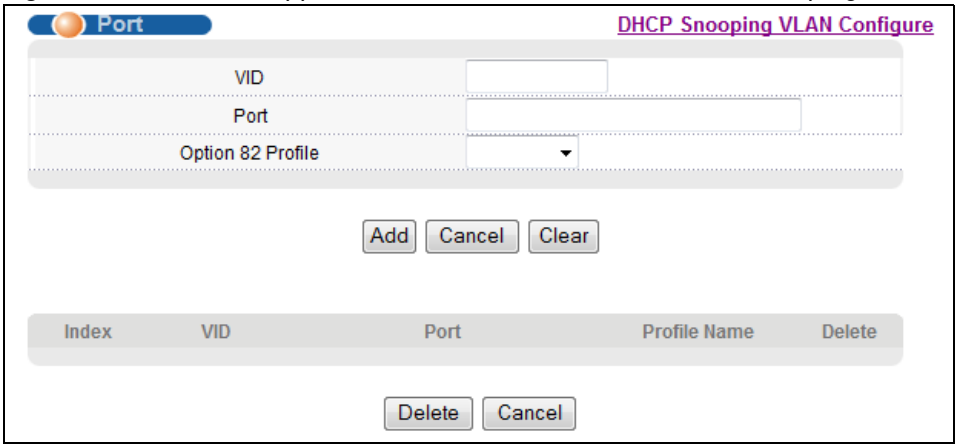
Table 103 Advanced Application > IP Source Guard > DHCP Snooping > Configure > VLAN

LABEL	DESCRIPTION
Show VLAN	Use this section to specify the VLANs you want to manage in the section below.
Start VID	Enter the lowest VLAN ID you want to manage in the section below.
End VID	Enter the highest VLAN ID you want to manage in the section below.
Apply	Click this to display the specified range of VLANs in the section below.
VID	This field displays the VLAN ID of each VLAN in the range specified above. If you configure the ***** VLAN, the settings are applied to all VLANs.
Enabled	Select **Yes** to enable DHCP snooping on the VLAN. You still have to enable DHCP snooping on the Switch and specify trusted ports. Note: If DHCP is enabled and there are no trusted ports, DHCP requests will not succeed.
Option 82 Profile	Select a pre-defined DHCP option 82 profile that the Switch applies to all ports in the specified VLAN(s). The Switch adds the information (such as slot number, port number, VLAN ID and/or system name) specified in the profile to DHCP requests that it broadcasts to the DHCP VLAN, if specified, or VLAN. You can specify the DHCP VLAN in the **DHCP Snooping Configure** screen (see Section 26.5 on page 218).
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values in this screen to their last-saved values.

26.5.3 DHCP Snooping VLAN Port Configure

Use this screen to apply a different DHCP option 82 profile to certain ports in a VLAN. To open this screen, click **Advanced Application > IP Source Guard > DHCP Snooping > Configure > VLAN > Port.**

Figure 154 Advanced Application > IP Source Guard > DHCP Snooping > Configure > VLAN > Port



The following table describes the labels in this screen.

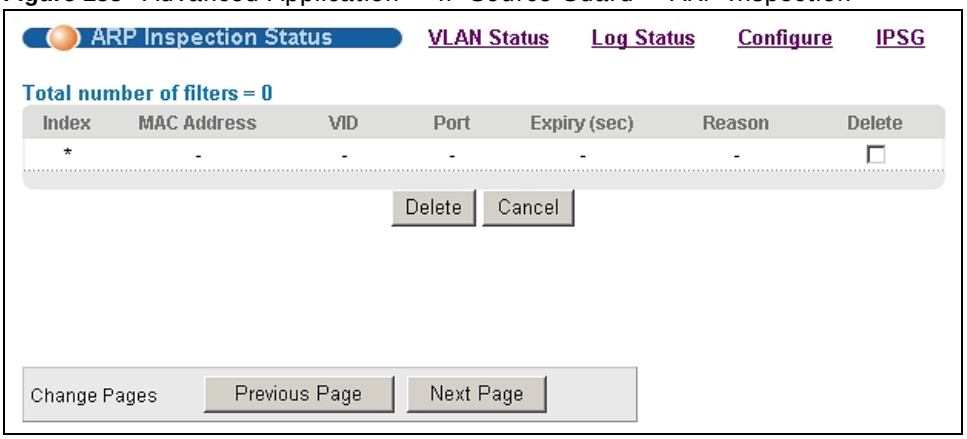
Table 104 Advanced Application > IP Source Guard > DHCP Snooping > Configure > VLAN > Port

LABEL	DESCRIPTION
VID	Enter the ID number of the VLAN you want to configure here.
Port	Enter the number of port(s) to which you want to apply the specified DHCP option 82 profile. You can enter multiple ports separated by (no space) comma (,) or hyphen (-). For example, enter “3-5” for ports 3, 4, and 5. Enter “3,5,7” for ports 3, 5, and 7.
Option 82 Profile	Select a pre-defined DHCP option 82 profile that the Switch applies to the specified port(s) in this VLAN. The Switch adds the information (such as slot number, port number, VLAN ID and/or system name) specified in the profile to DHCP requests that it broadcasts to the DHCP VLAN, if specified, or VLAN. You can specify the DHCP VLAN in the **DHCP Snooping Configure** screen (see Section 26.5 on page 218). The profile you select here has priority over the one you select in the **DHCP Snooping > Configure > VLAN** screen.
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch’s run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values above based on the last selected entry or, if not applicable, to clear the fields above.
Clear	Click **Clear** to reset the fields to the factory defaults.
Index	This field displays a sequential number for each entry. Click an index number to change the settings.
VID	This field displays the VLAN to which the port(s) belongs.
Port	This field displays the port(s) to which the Switch applies the settings.
Profile Name	This field displays the DHCP option 82 profile that the Switch applies to the port(s).
Delete	Select the entry(ies) that you want to remove in the **Delete** column, then click the **Delete** button to remove the selected entry(ies) from the table.
Delete	Click this to remove the selected entry(ies) from the table.
Cancel	Click this to clear the **Delete** check boxes above.

26.6 ARP Inspection Status

Use this screen to look at the current list of MAC address filters that were created because the Switch identified an unauthorized ARP packet. When the Switch identifies an unauthorized ARP packet, it automatically creates a MAC address filter to block traffic from the source MAC address and source VLAN ID of the unauthorized ARP packet. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection**.

Figure 155 Advanced Application > IP Source Guard > ARP Inspection



The following table describes the labels in this screen.

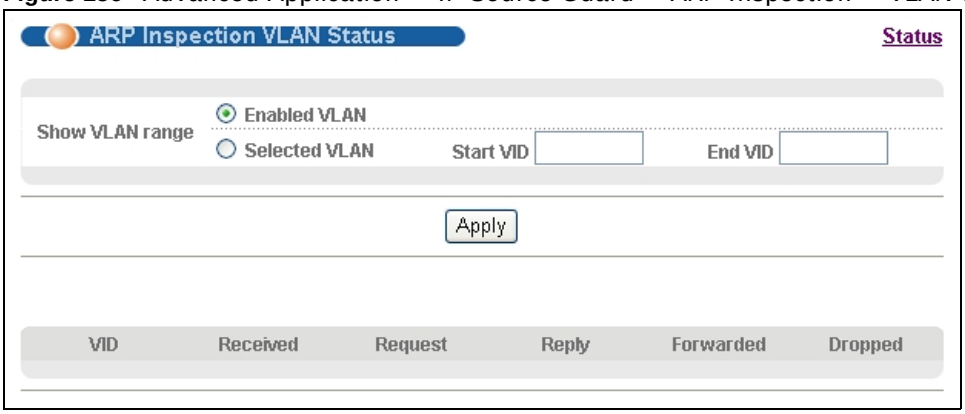
Table 105 Advanced Application > IP Source Guard > ARP Inspection

LABEL	DESCRIPTION
Total number of filters	This field displays the current number of MAC address filters that were created because the Switch identified unauthorized ARP packets.
Index	This field displays a sequential number for each MAC address filter.
MAC Address	This field displays the source MAC address in the MAC address filter.
VID	This field displays the source VLAN ID in the MAC address filter.
Port	This field displays the source port of the discarded ARP packet.
Expiry (sec)	This field displays how long (in seconds) the MAC address filter remains in the Switch. You can also delete the record manually (**Delete**).
Reason	This field displays the reason the ARP packet was discarded. **MAC+VLAN**: The MAC address and VLAN ID were not in the binding table. **IP**: The MAC address and VLAN ID were in the binding table, but the IP address was not valid. **Port**: The MAC address, VLAN ID, and IP address were in the binding table, but the port number was not valid.
Delete	Select this, and click **Delete** to remove the specified entry.
Cancel	Click this to clear the **Delete** check boxes above.
Change Pages	Click **Previous** or **Next** to show the previous/next screen if all status information cannot be seen in one screen.

26.7 ARP Inspection VLAN Status

Use this screen to look at various statistics about ARP packets in each VLAN. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection > VLAN Status**.

Figure 156 Advanced Application > IP Source Guard > ARP Inspection > VLAN Status



The following table describes the labels in this screen.

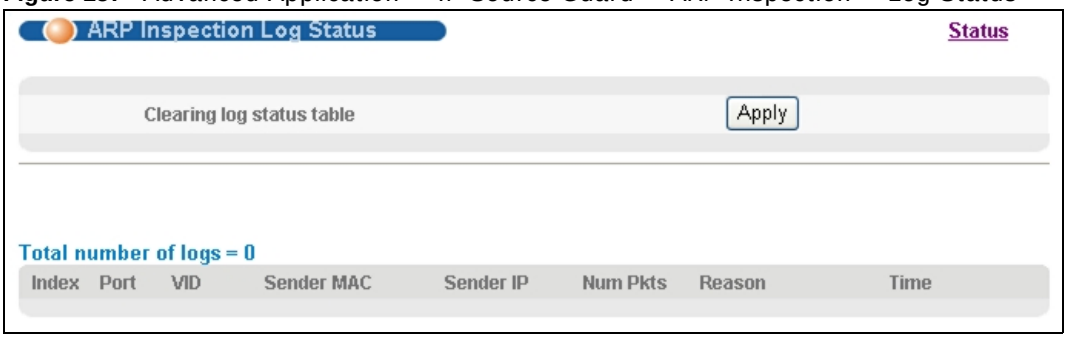
Table 106 Advanced Application > IP Source Guard > ARP Inspection > VLAN Status

LABEL	DESCRIPTION
Show VLAN range	Use this section to specify the VLANs you want to look at in the section below.
Enabled VLAN	Select this to look at all the VLANs on which ARP inspection is enabled in the section below.
Selected VLAN	Select this to look at all the VLANs in a specific range in the section below. Then, enter the lowest VLAN ID (**Start VID**) and the highest VLAN ID (**End VID**) you want to look at.
Apply	Click this to display the specified range of VLANs in the section below.
VID	This field displays the VLAN ID of each VLAN in the range specified above.
Received	This field displays the total number of ARP packets received from the VLAN since the Switch last restarted.
Request	This field displays the total number of ARP Request packets received from the VLAN since the Switch last restarted.
Reply	This field displays the total number of ARP Reply packets received from the VLAN since the Switch last restarted.
Forwarded	This field displays the total number of ARP packets the Switch forwarded for the VLAN since the Switch last restarted.
Dropped	This field displays the total number of ARP packets the Switch discarded for the VLAN since the Switch last restarted.

26.8 ARP Inspection Log Status

Use this screen to look at log messages that were generated by ARP packets and that have not been sent to the syslog server yet. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection > Log Status**.

Figure 157 Advanced Application > IP Source Guard > ARP Inspection > Log Status



The following table describes the labels in this screen.

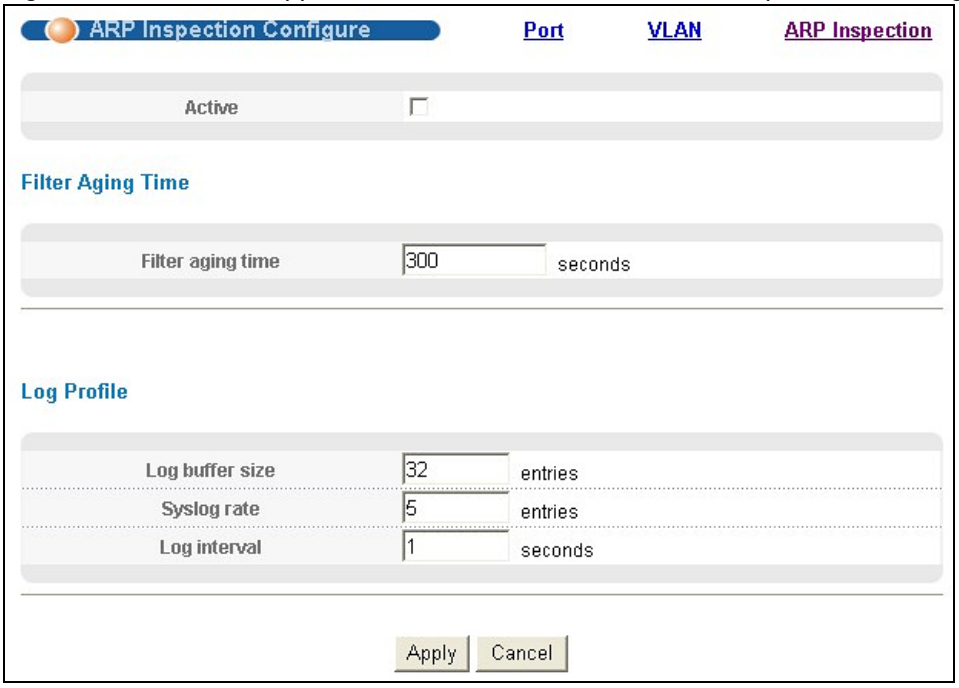
Table 107 Advanced Application > IP Source Guard > ARP Inspection > Log Status

LABEL	DESCRIPTION
Clearing log status table	Click **Apply** to remove all the log messages that were generated by ARP packets and that have not been sent to the syslog server yet.
Total number of logs	This field displays the number of log messages that were generated by ARP packets and that have not been sent to the syslog server yet. If one or more log messages are dropped due to unavailable buffer, there is an entry called **overflow** with the current number of dropped log messages.
Index	This field displays a sequential number for each log message.
Port	This field displays the source port of the ARP packet.
VID	This field displays the source VLAN ID of the ARP packet.
Sender MAC	This field displays the source MAC address of the ARP packet.
Sender IP	This field displays the source IP address of the ARP packet.
Num Pkts	This field displays the number of ARP packets that were consolidated into this log message. The Switch consolidates identical log messages generated by ARP packets in the log consolidation interval into one log message. You can configure this interval in the **ARP Inspection Configure** screen. See Section 26.9 on page 227.
Reason	This field displays the reason the log message was generated. **dhcp deny**: An ARP packet was discarded because it violated a dynamic binding with the same MAC address and VLAN ID. **static deny**: An ARP packet was discarded because it violated a static binding with the same MAC address and VLAN ID. **deny**: An ARP packet was discarded because there were no bindings with the same MAC address and VLAN ID. **dhcp permit**: An ARP packet was forwarded because it matched a dynamic binding. **static permit**: An ARP packet was forwarded because it matched a static binding. In the **ARP Inspection VLAN Configure** screen, you can configure the Switch to generate log messages when ARP packets are discarded or forwarded based on the VLAN ID of the ARP packet. See Section 26.9.2 on page 230.
Time	This field displays when the log message was generated.

26.9 ARP Inspection Configure

Use this screen to enable ARP inspection on the Switch. You can also configure the length of time the Switch stores records of discarded ARP packets and global settings for the ARP inspection log. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection > Configure**.

Figure 158 Advanced Application > IP Source Guard > ARP Inspection > Configure



The following table describes the labels in this screen.

Table 108 Advanced Application > IP Source Guard > ARP Inspection > Configure

LABEL	DESCRIPTION
Active	Select this to enable ARP inspection on the Switch. You still have to enable ARP inspection on specific VLAN and specify trusted ports.
Filter Aging Time	
Filter aging time	This setting has no effect on existing MAC address filters. Enter how long (1~2147483647 seconds) the MAC address filter remains in the Switch after the Switch identifies an unauthorized ARP packet. The Switch automatically deletes the MAC address filter afterwards. Enter 0 if you want the MAC address filter to be permanent.
Log Profile	
Log buffer size	Enter the maximum number (1~1024) of log messages that were generated by ARP packets and have not been sent to the syslog server yet. Make sure this number is appropriate for the specified **Syslog rate** and **Log interval**. If the number of log messages in the Switch exceeds this number, the Switch stops recording log messages and simply starts counting the number of entries that were dropped due to unavailable buffer. Click **Clearing log status table** in the **ARP Inspection Log Status** screen to clear the log and reset this counter. See Section 26.8 on page 225.

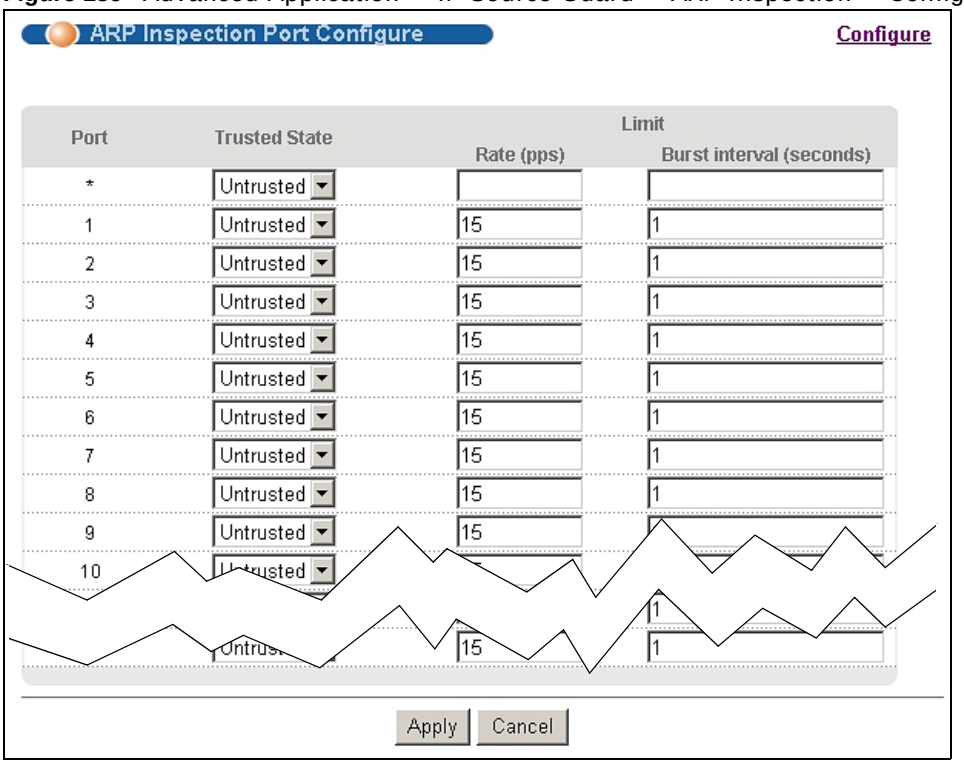
Table 108 Advanced Application > IP Source Guard > ARP Inspection > Configure (continued)

LABEL	DESCRIPTION
Syslog rate	Enter the maximum number of syslog messages the Switch can send to the syslog server in one batch. This number is expressed as a rate because the batch frequency is determined by the **Log Interval**. You must configure the syslog server (Chapter 42 on page 346) to use this. Enter 0 if you do not want the Switch to send log messages generated by ARP packets to the syslog server. The relationship between **Syslog rate** and **Log interval** is illustrated in the following examples: • 4 invalid ARP packets per second, **Syslog rate** is 5, **Log interval** is 1: the Switch sends 4 syslog messages every second. • 6 invalid ARP packets per second, **Syslog rate** is 5, **Log interval** is 2: the Switch sends 5 syslog messages every 2 seconds.
Log interval	Enter how often (1-86400 seconds) the Switch sends a batch of syslog messages to the syslog server. Enter 0 if you want the Switch to send syslog messages immediately. See **Syslog rate** for an example of the relationship between **Syslog rate** and **Log interval**.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values in this screen to their last-saved values.

26.9.1 ARP Inspection Port Configure

Use this screen to specify whether ports are trusted or untrusted ports for ARP inspection. You can also specify the maximum rate at which the Switch receives ARP packets on each untrusted port. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection > Configure > Port**.

Figure 159 Advanced Application > IP Source Guard > ARP Inspection > Configure > Port



The following table describes the labels in this screen.

Table 109 Advanced Application > IP Source Guard > ARP Inspection > Configure > Port

LABEL	DESCRIPTION
Port	This field displays the port number. If you configure the ***** port, the settings are applied to all of the ports.
Trusted State	Select whether this port is a trusted port (**Trusted**) or an untrusted port (**Untrusted**). The Switch does not discard ARP packets on trusted ports for any reason. The Switch discards ARP packets on untrusted ports in the following situations: • The sender's information in the ARP packet does not match any of the current bindings. • The rate at which ARP packets arrive is too high. You can specify the maximum rate at which ARP packets can arrive on untrusted ports.
Limit	These settings have no effect on trusted ports.
Rate (pps)	Specify the maximum rate (1-2048 packets per second) at which the Switch receives ARP packets from each port. The Switch discards any additional ARP packets. Enter 0 to disable this limit.
Burst interval (seconds)	The burst interval is the length of time over which the rate of ARP packets is monitored for each port. For example, if the rate is 15 pps and the burst interval is 1 second, then the Switch accepts a maximum of 15 ARP packets in every one-second interval. If the burst interval is 5 seconds, then the Switch accepts a maximum of 75 ARP packets in every five-second interval. Enter the length (1-15 seconds) of the burst interval.

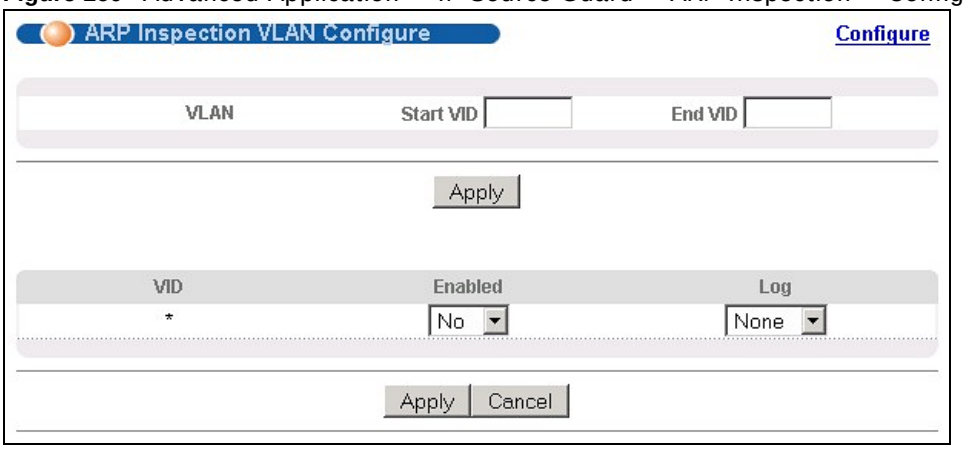
Table 109 Advanced Application > IP Source Guard > ARP Inspection > Configure > Port

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values in this screen to their last-saved values.

26.9.2 ARP Inspection VLAN Configure

Use this screen to enable ARP inspection on each VLAN and to specify when the Switch generates log messages for receiving ARP packets from each VLAN. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection > Configure > VLAN**.

Figure 160 Advanced Application > IP Source Guard > ARP Inspection > Configure > VLAN



The following table describes the labels in this screen.

Table 110 Advanced Application > IP Source Guard > ARP Inspection > Configure > VLAN

LABEL	DESCRIPTION
VLAN	Use this section to specify the VLANs you want to manage in the section below.
Start VID	Enter the lowest VLAN ID you want to manage in the section below.
End VID	Enter the highest VLAN ID you want to manage in the section below.
Apply	Click this to display the specified range of VLANs in the section below.
VID	This field displays the VLAN ID of each VLAN in the range specified above. If you configure the ***** VLAN, the settings are applied to all VLANs.
Enabled	Select **Yes** to enable ARP inspection on the VLAN. Select **No** to disable ARP inspection on the VLAN.

Table 110 Advanced Application > IP Source Guard > ARP Inspection > Configure > VLAN

LABEL	DESCRIPTION
Log	Specify when the Switch generates log messages for receiving ARP packets from the VLAN. **None**: The Switch does not generate any log messages when it receives an ARP packet from the VLAN. **Deny**: The Switch generates log messages when it discards an ARP packet from the VLAN. **Permit**: The Switch generates log messages when it forwards an ARP packet from the VLAN. **All**: The Switch generates log messages every time it receives an ARP packet from the VLAN.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values in this screen to their last-saved values.

26.10 Technical Reference

This section provides technical background information on the topics discussed in this chapter.

26.10.1 DHCP Snooping Overview

Use DHCP snooping to filter unauthorized DHCP packets on the network and to build the binding table dynamically. This can prevent clients from getting IP addresses from unauthorized DHCP servers.

26.10.1.1 Trusted vs. Untrusted Ports

Every port is either a trusted port or an untrusted port for DHCP snooping. This setting is independent of the trusted/untrusted setting for ARP inspection. You can also specify the maximum number for DHCP packets that each port (trusted or untrusted) can receive each second.

Trusted ports are connected to DHCP servers or other switches. The Switch discards DHCP packets from trusted ports only if the rate at which DHCP packets arrive is too high. The Switch learns dynamic bindings from trusted ports.

Note: If DHCP is enabled and there are no trusted ports, DHCP requests will not succeed.

Untrusted ports are connected to subscribers. The Switch discards DHCP packets from untrusted ports in the following situations:

- The packet is a DHCP server packet (for example, OFFER, ACK, or NACK).
- The source MAC address and source IP address in the packet do not match any of the current bindings.
- The packet is a RELEASE or DECLINE packet, and the source MAC address and source port do not match any of the current bindings.
- The rate at which DHCP packets arrive is too high.

26.10.1.2 DHCP Snooping Database

The Switch stores the binding table in volatile memory. If the Switch restarts, it loads static bindings from permanent memory but loses the dynamic bindings, in which case the devices in the network have to send DHCP requests again. As a result, it is recommended you configure the DHCP snooping database.

The DHCP snooping database maintains the dynamic bindings for DHCP snooping and ARP inspection in a file on an external TFTP server. If you set up the DHCP snooping database, the Switch can reload the dynamic bindings from the DHCP snooping database after the Switch restarts.

You can configure the name and location of the file on the external TFTP server. The file has the following format:

Figure 161 DHCP Snooping Database File Format

```
<initial-checksum>
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
<binding-1> <checksum-1>
<binding-2> <checksum-1-2>
...
...
<binding-n> <checksum-1-2-..-n>
END
```

The <initial-checksum> helps distinguish between the bindings in the latest update and the bindings from previous updates. Each binding consists of 72 bytes, a space, and another checksum that is used to validate the binding when it is read. If the calculated checksum is not equal to the checksum in the file, that binding and all others after it are ignored.

26.10.1.3 DHCP Relay Option 82 Information

The Switch can add information to DHCP requests that it does not discard. This provides the DHCP server more information about the source of the requests. The Switch can add the following information:

- Slot ID (1 byte), port ID (1 byte), and source VLAN ID (2 bytes)
- System name (up to 32 bytes)

This information is stored in an Agent Information field in the option 82 field of the DHCP headers of client DHCP request frames. See Chapter 37 on page 300 for more information about DHCP relay option 82.

When the DHCP server responds, the Switch removes the information in the Agent Information field before forwarding the response to the original source.

You can configure this setting for each source VLAN. This setting is independent of the DHCP relay settings (Chapter 37 on page 300).

26.10.1.4 Configuring DHCP Snooping

Follow these steps to configure DHCP snooping on the Switch.

1 Enable DHCP snooping on the Switch.

2 Enable DHCP snooping on each VLAN, and configure DHCP relay option 82.

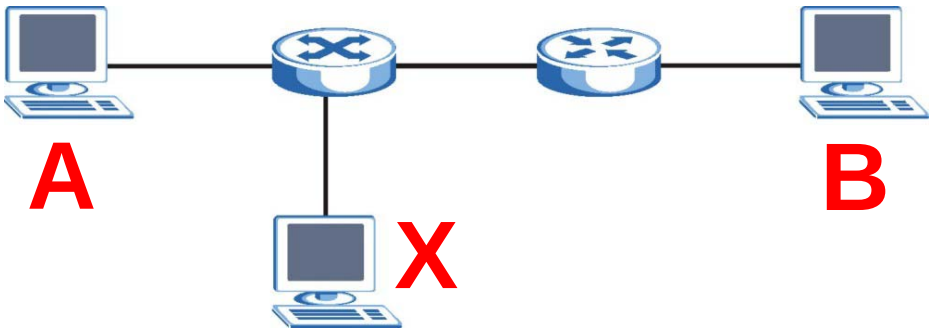
3 Configure trusted and untrusted ports, and specify the maximum number of DHCP packets that each port can receive per second.

4 Configure static bindings.

26.10.2 ARP Inspection Overview

Use ARP inspection to filter unauthorized ARP packets on the network. This can prevent many kinds of man-in-the-middle attacks, such as the one in the following example.

Figure 162 Example: Man-in-the-middle Attack



In this example, computer **B** tries to establish a connection with computer **A**. Computer **X** is in the same broadcast domain as computer **A** and intercepts the ARP request for computer **A**. Then, computer **X** does the following things:

- It pretends to be computer **A** and responds to computer **B**.
- It pretends to be computer **B** and sends a message to computer **A**.

As a result, all the communication between computer **A** and computer **B** passes through computer **X**. Computer **X** can read and alter the information passed between them.

26.10.2.1 ARP Inspection and MAC Address Filters

When the Switch identifies an unauthorized ARP packet, it automatically creates a MAC address filter to block traffic from the source MAC address and source VLAN ID of the unauthorized ARP packet. You can configure how long the MAC address filter remains in the Switch.

These MAC address filters are different than regular MAC address filters (Chapter 12 on page 113).

- They are stored only in volatile memory.
- They do not use the same space in memory that regular MAC address filters use.
- They appear only in the **ARP Inspection** screens, not in the **MAC Address Filter** screens.

26.10.2.2 Trusted vs. Untrusted Ports

Every port is either a trusted port or an untrusted port for ARP inspection. This setting is independent of the trusted/untrusted setting for DHCP snooping. You can also specify the maximum rate at which the Switch receives ARP packets on untrusted ports.

The Switch does not discard ARP packets on trusted ports for any reason.

The Switch discards ARP packets on untrusted ports in the following situations:

- The sender's information in the ARP packet does not match any of the current bindings.
- The rate at which ARP packets arrive is too high.

26.10.2.3 Syslog

The Switch can send syslog messages to the specified syslog server (Chapter 42 on page 346) when it forwards or discards ARP packets. The Switch can consolidate log messages and send log messages in batches to make this mechanism more efficient.

26.10.2.4 Configuring ARP Inspection

Follow these steps to configure ARP inspection on the Switch.

1. Configure DHCP snooping. See Section 26.10.1.4 on page 232.

   Note: It is recommended you enable DHCP snooping at least one day before you enable ARP inspection so that the Switch has enough time to build the binding table.

2. Enable ARP inspection on each VLAN.

3. Configure trusted and untrusted ports, and specify the maximum number of ARP packets that each port can receive per second.

27

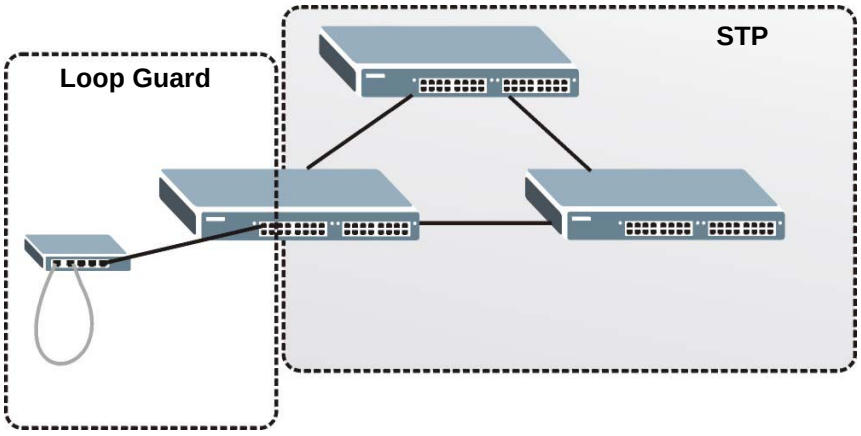
Loop Guard

27.1 Loop Guard Overview

This chapter shows you how to configure the Switch to guard against loops on the edge of your network.

Loop guard allows you to configure the Switch to shut down a port if it detects that packets sent out on that port loop back to the Switch. While you can use Spanning Tree Protocol (STP) to prevent loops in the core of your network. STP cannot prevent loops that occur on the edge of your network.

Figure 163 Loop Guard vs. STP



Refer to Section 27.1.2 on page 235 for more information.

27.1.1 What You Can Do

Use the **Loop Guard** screen (Section 27.2 on page 237) to enable loop guard on the Switch and in specific ports.

27.1.2 What You Need to Know

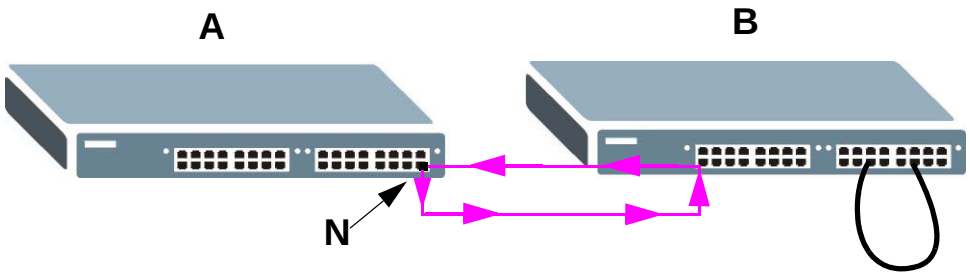
Loop guard is designed to handle loop problems on the edge of your network. This can occur when a port is connected to a Switch that is in a loop state. Loop state occurs as a result of human error. It happens when two ports on a switch are connected with the same cable. When a switch in loop state sends out broadcast messages the messages loop back to the switch and are re-broadcast again and again causing a broadcast storm.

If a switch (not in loop state) connects to a switch in loop state, then it will be affected by the switch in loop state in the following way:

- It will receive broadcast messages sent out from the switch in loop state.
- It will receive its own broadcast messages that it sends out as they loop back. It will then re-broadcast those messages again.

The following figure shows port **N** on switch **A** connected to switch **B**. Switch **B** is in loop state. When broadcast or multicast packets leave port **N** and reach switch **B**, they are sent back to port **N** on **A** as they are rebroadcast from B.

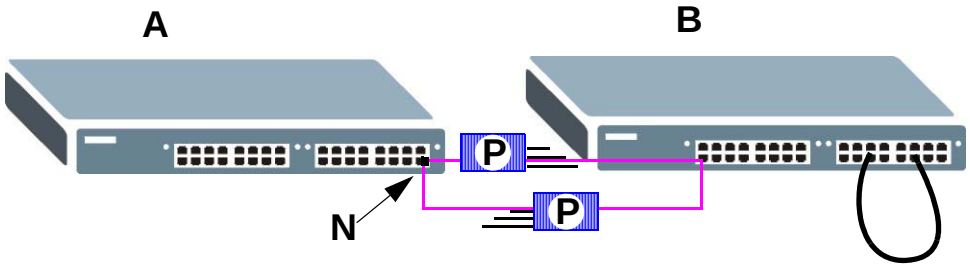
Figure 164 Switch in Loop State



The loop guard feature checks to see if a loop guard enabled port is connected to a switch in loop state. This is accomplished by periodically sending a probe packet and seeing if the packet returns on the same port. If this is the case, the Switch will shut down the port connected to the switch in loop state.

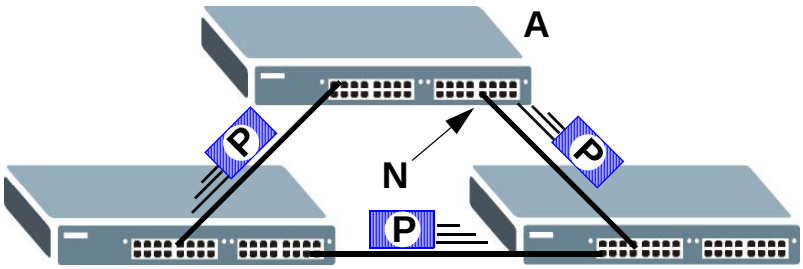
The following figure shows a loop guard enabled port **N** on switch **A** sending a probe packet **P** to switch **B**. Since switch **B** is in loop state, the probe packet **P** returns to port **N** on **A**. The Switch then shuts down port **N** to ensure that the rest of the network is not affected by the switch in loop state.

Figure 165 Loop Guard - Probe Packet



The Switch also shuts down port **N** if the probe packet returns to switch **A** on any other port. In other words loop guard also protects against standard network loops. The following figure illustrates three switches forming a loop. A sample path of the loop guard probe packet is also shown. In this example, the probe packet is sent from port **N** and returns on another port. As long as loop guard is enabled on port **N**. The Switch will shut down port **N** if it detects that the probe packet has returned to the Switch.

Figure 166 Loop Guard - Network Loop



Note: After resolving the loop problem on your network you can re-activate the disabled port via the web configurator (see Section 8.7 on page 69).

27.2 Loop Guard Setup

Click **Advanced Application** > **Loop Guard** in the navigation panel to display the screen as shown.

Note: The loop guard feature can not be enabled on the ports that have Spanning Tree Protocol (RSTP, MRSTP or MSTP) enabled.

Figure 167 Advanced Application > Loop Guard

The following table describes the labels in this screen.

Table 111 Advanced Application > Loop Guard

LABEL	DESCRIPTION
Active	Select this option to enable loop guard on the Switch. The Switch generates syslog, internal log messages as well as SNMP traps when it shuts down a port via the loop guard feature.
Port	This field displays the port number.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to enable the loop guard feature on this port. The Switch sends probe packets from this port to check if the switch it is connected to is in loop state. If the switch that this port is connected is in loop state the Switch will shut down this port. Clear this check box to disable the loop guard feature.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

28

Layer 2 Protocol Tunneling

28.1 Layer 2 Protocol Tunneling Overview

This chapter shows you how to configure layer 2 protocol tunneling on the Switch.

Layer 2 protocol tunneling (L2PT) is used on the service provider's edge devices.

28.1.1 What You Can Do

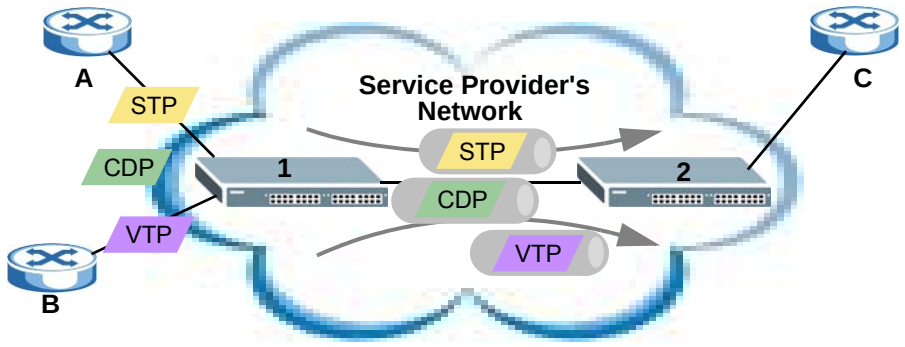
Use the **Layer 2 Protocol Tunnel** screen (Section 28.2 on page 240) to enable layer 2 protocol tunneling on the Switch and specify a MAC address with which the Switch uses to encapsulate the layer 2 protocol packets by replacing the destination MAC address in the packets.

28.1.2 What You Need to Know

Layer 2 protocol tunneling (L2PT) is used on the service provider's edge devices.

L2PT allows edge switches (**1** and **2** in the following figure) to tunnel layer 2 STP (Spanning Tree Protocol), CDP (Cisco Discovery Protocol) and VTP (VLAN Trunking Protocol) packets between customer switches (**A**, **B** and **C** in the following figure) connected through the service provider's network. The edge switch encapsulates layer 2 protocol packets with a specific MAC address before sending them across the service provider's network to other edge switches.

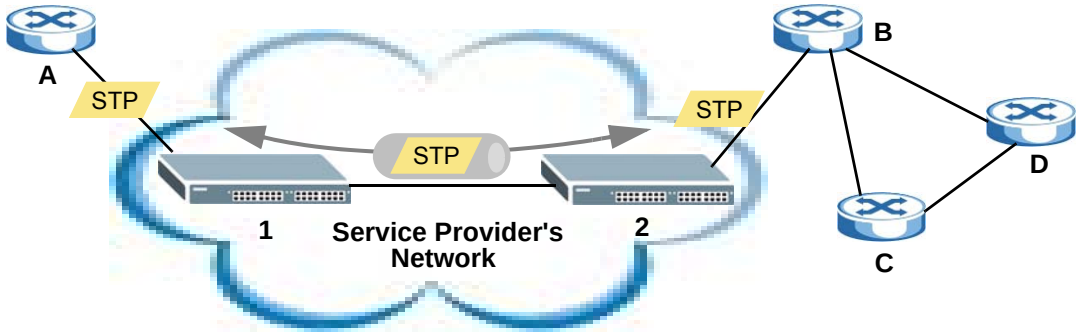
Figure 168 Layer 2 Protocol Tunneling Network Scenario



In the following example, if you enable L2PT for STP, you can have switches **A**, **B**, **C** and **D** in the same spanning tree, even though switch **A** is not directly connected to switches **B**, **C** and **D**. Topology change information can be propagated throughout the service provider's network.

To emulate a point-to-point topology between two customer switches at different sites, such as **A** and **B**, you can enable protocol tunneling on edge switches **1** and **2** for PAgP (Port Aggregation Protocol), LACP or UDLD (UniDirectional Link Detection).

Figure 169 L2PT Network Example



28.1.2.1 Layer 2 Protocol Tunneling Mode

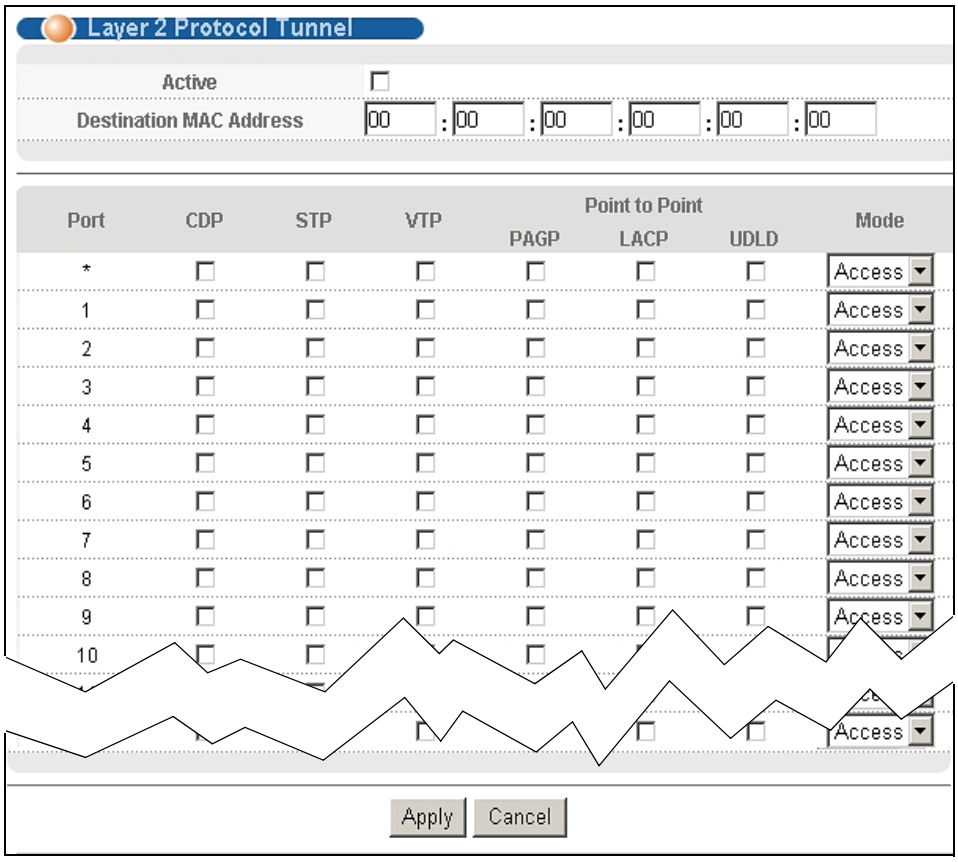
Each port can have two layer 2 protocol tunneling modes, **Access** and **Tunnel**.

- The **Access** port is an ingress port on the service provider's edge device (**1** or **2** in Figure 169 on page 240) and connected to a customer switch (**A** or **B**). Incoming layer 2 protocol packets received on an access port are encapsulated and forwarded to the tunnel ports.
- The **Tunnel** port is an egress port at the edge of the service provider's network and connected to another service provider's switch. Incoming encapsulated layer 2 protocol packets received on a tunnel port are decapsulated and sent to an access port.

28.2 Configuring Layer 2 Protocol Tunneling

Click **Advanced Application** > **Layer 2 Protocol Tunneling** in the navigation panel to display the screen as shown.

Figure 170 Advanced Application > Layer 2 Protocol Tunneling



The following table describes the labels in this screen.

Table 112 Advanced Application > Layer 2 Protocol Tunneling

LABEL	DESCRIPTION
Active	Select this to enable layer 2 protocol tunneling on the Switch.
Destination MAC Address	Specify a MAC address with which the Switch uses to encapsulate the layer 2 protocol packets by replacing the destination MAC address in the packets. Note: The MAC address can be either a unicast MAC address or multicast MAC address. If you use a unicast MAC address, make sure the MAC address does not exist in the address table of a switch on the service provider's network. Note: All the edge switches in the service provider's network should be set to use the same MAC address for encapsulation.
Port	This field displays the port number.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
CDP	Select this option to have the Switch tunnel CDP (Cisco Discovery Protocol) packets so that other Cisco devices can be discovered through the service provider's network.
STP	Select this option to have the Switch tunnel STP (Spanning Tree Protocol) packets so that STP can run properly across the service provider's network and spanning trees can be set up based on bridge information from all (local and remote) networks.

Table 112 Advanced Application > Layer 2 Protocol Tunneling (continued)

LABEL	DESCRIPTION
VTP	Select this option to have the Switch tunnel VTP (VLAN Trunking Protocol) packets so that all customer switches can use consistent VLAN configuration through the service provider's network.
Point to Point	The Switch supports PAgP (Port Aggregation Protocol), LACP (Link Aggregation Control Protocol) and UDLD (UniDirectional Link Detection) tunneling for a point-to-point topology. Both PAgP and UDLD are Cisco's proprietary data link layer protocols. PAgP is similar to LACP and used to set up a logical aggregation of Ethernet ports automatically. UDLD is to determine the link's physical status and detect a unidirectional link.
PAGP	Select this option to have the Switch send PAgP packets to a peer to automatically negotiate and build a logical port aggregation.
LACP	Select this option to have the Switch send LACP packets to a peer to dynamically creates and manages trunk groups.
UDLD	Select this option to have the Switch send UDLD packets to a peer's port it connected to monitor the physical status of a link.
Mode	Select **Access** to have the Switch encapsulate the incoming layer 2 protocol packets and forward them to the tunnel port(s). Select **Access** for ingress ports at the edge of the service provider's network. Note: You can enable L2PT services for STP, LACP, VTP, CDP, UDLD, and PAGP on the access port(s) only. Select **Tunnel** for egress ports at the edge of the service provider's network. The Switch decapsulates the encapsulated layer 2 protocol packets received on a tunnel port by changing the destination MAC address to the original one, and then forward them to an access port. If the service(s) is not enabled on an access port, the protocol packets are dropped.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

29

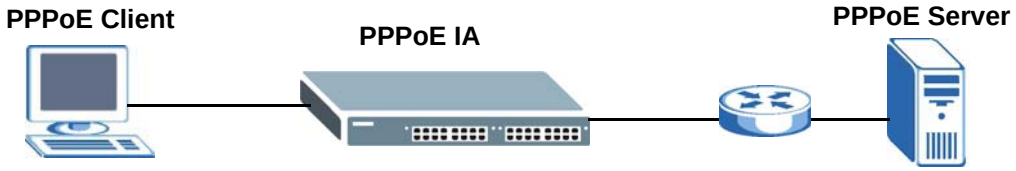
PPPoE

29.1 PPPoE Intermediate Agent Overview

This chapter describes how the Switch gives a PPPoE termination server additional information that the server can use to identify and authenticate a PPPoE client.

A PPPoE Intermediate Agent (PPPoE IA) is deployed between a PPPoE server and PPPoE clients. It helps the PPPoE server identify and authenticate clients by adding subscriber line specific information to PPPoE discovery packets from clients on a per-port or per-port-per-VLAN basis before forwarding them to the PPPoE server.

Figure 171 PPPoE Intermediate Agent (PPPoE IA) Overview



29.1.1 What You Can Do

- Use the **PPPoE** screen (Section 29.2 on page 246) to display the main PPPoE screen.
- Use the **Intermediate Agent** screen (Section 29.3 on page 246) to enable the PPPoE Intermediate Agent on the Switch.
- Use the **PPPoE IA Per-Port** screen (Section 29.3.1 on page 247) to set the port state and configure PPPoE intermediate agent sub-options on a per-port basis.
- Use the **PPPoE IA Per-Port Per-VLAN** screen (Section 29.3.2 on page 249) to configure PPPoE IA settings that apply to a specific VLAN on a port.
- Use the **PPPoE IA for VLAN** (Section 29.3.3 on page 250) to enable the PPPoE Intermediate Agent on a VLAN.

29.1.2 What You Need to Know

Read on for concepts on ARP that can help you configure the screen in this chapter.

29.1.2.1 PPPoE Intermediate Agent Tag Format

If the PPPoE Intermediate Agent is enabled, the Switch adds a vendor-specific tag to PADI (PPPoE Active Discovery Initialization) and PADR (PPPoE Active Discovery Request) packets from PPPoE clients. This tag is defined in RFC 2516 and has the following format for this feature.

Table 113 PPPoE Intermediate Agent Vendor-specific Tag Format

Tag_Type (0x0105)	Tag_Len	Value	i1	i2

The Tag_Type is 0x0105 for vendor-specific tags, as defined in RFC 2516. The Tag_Len indicates the length of Value, i1 and i2. The Value is the 32-bit number 0x00000DE9, which stands for the “ADSL Forum” IANA entry. i1 and i2 are PPPoE intermediate agent sub-options, which contain additional information about the PPPoE client.

29.1.2.2 Sub-Option Format

There are two types of sub-option: “Agent Circuit ID Sub-option” and “Agent Remote ID Sub-option”. They have the following formats.

Table 114 PPPoE IA Circuit ID Sub-option Format: User-defined String

SubOpt	Length	Value
0x01 (1 byte)	N (1 byte)	String (63 bytes)

Table 115 PPPoE IA Remote ID Sub-option Format

SubOpt	Length	Value
0x02 (1 byte)	N (1 byte)	MAC Address or String (63 bytes)

The 1 in the first field identifies this as an Agent Circuit ID sub-option and 2 identifies this as an Agent Remote ID sub-option. The next field specifies the length of the field. The Switch takes the Circuit ID string you manually configure for a VLAN on a port as the highest priority and the Circuit ID string for a port as the second priority. In addition, the Switch puts the PPPoE client’s MAC address into the Agent Remote ID Sub-option if you do not specify any user-defined string.

Flexible Circuit ID Syntax with Identifier String and Variables

If you do not configure a Circuit ID string for a VLAN on a specific port or for a specific port, the Switch adds the user-defined identifier string and variables into the Agent Circuit ID Sub-option. The variables can be the slot ID of the PPPoE client, the port number of the PPPoE client and/or the VLAN ID on the PPPoE packet.

The identifier-string, slot ID, port number and VLAN ID are separated from each other by a pound key (#), semi-colon (;), period (.), comma (,), forward slash (/) or space. An Agent Circuit ID Sub-

option example is “Switch/07/0123” and indicates the PPPoE packets come from a PPPoE client which is connected to the Switch’s port 7 and belong to VLAN 123.

Table 116 PPPoE IA Circuit ID Sub-option Format: Using Identifier String and Variables

SubOpt	Length	Value						
0x01 (1 byte)	N (1 byte)	Identifier String (53 byte)	delimiter (1 byte)	Slot ID (1 byte)	delimiter (1 byte)	Port No (2 byte)	delimiter (1 byte)	VLAN ID (4 bytes)

WT-101 Default Circuit ID Syntax

If you do not configure a Circuit ID string for a specific VLAN on a port or for a specific port, and disable the flexible Circuit ID syntax in the **PPPoE > Intermediate Agent** screen, the Switch automatically generates a Circuit ID string according to the default Circuit ID syntax which is defined in the DSL Forum Working Text (WT)-101. The default access node identifier is the host name of the PPPoE intermediate agent and the eth indicates “Ethernet”.

Table 117 PPPoE IA Circuit ID Sub-option Format: Defined in WT-101

SubOpt	Length	Value								
0x01 (1 byte)	N (1 byte)	Access Node Identifier (20 byte)	Space (1 byte)	eth (3 byte)	Space (1 byte)	Slot ID (1 byte)	/ (1 byte)	Port No (2 byte)	: (1 byte)	VLAN ID (4 bytes)

29.1.2.3 Port State

Every port is either a trusted port or an untrusted port for the PPPoE intermediate agent. This setting is independent of the trusted/untrusted setting for DHCP snooping or ARP inspection. You can also specify the agent sub-options (circuit ID and remote ID) that the Switch adds to PADI and PADR packets from PPPoE clients.

Trusted ports are connected to PPPoE servers.

- If a PADO (PPPoE Active Discovery Offer), PADS (PPPoE Active Discovery Session-confirmation), or PADT (PPPoE Active Discovery Terminate) packet is sent from a PPPoE server and received on a trusted port, the Switch forwards it to all other ports.
- If a PADI or PADR packet is sent from a PPPoE client but received on a trusted port, the Switch forwards it to other trusted port(s).

Note: The Switch will drop all PPPoE discovery packets if you enable the PPPoE intermediate agent and there are no trusted ports.

Untrusted ports are connected to subscribers.

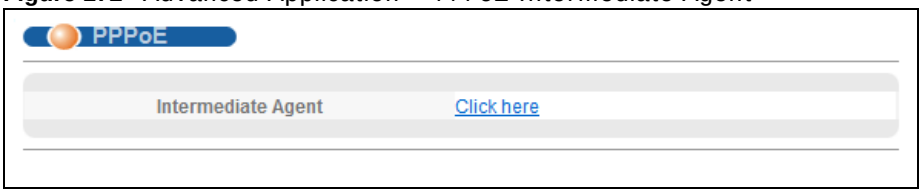
- If a PADI, PADR, or PADT packet is sent from a PPPoE client and received on an untrusted port, the Switch adds a vendor-specific tag to the packet and then forwards it to the trusted port(s).
- The Switch discards PADO and PADS packets which are sent from a PPPoE server but received on an untrusted port.

29.2 The PPPoE Screen

Use this screen to configure the PPPoE Intermediate Agent on the Switch.

Click **Advanced Application** > **PPPoE** in the navigation panel to display the screen as shown. Click **Click Here** to go to the **Intermediate Agent** screen.

Figure 172 Advanced Application > PPPoE Intermediate Agent

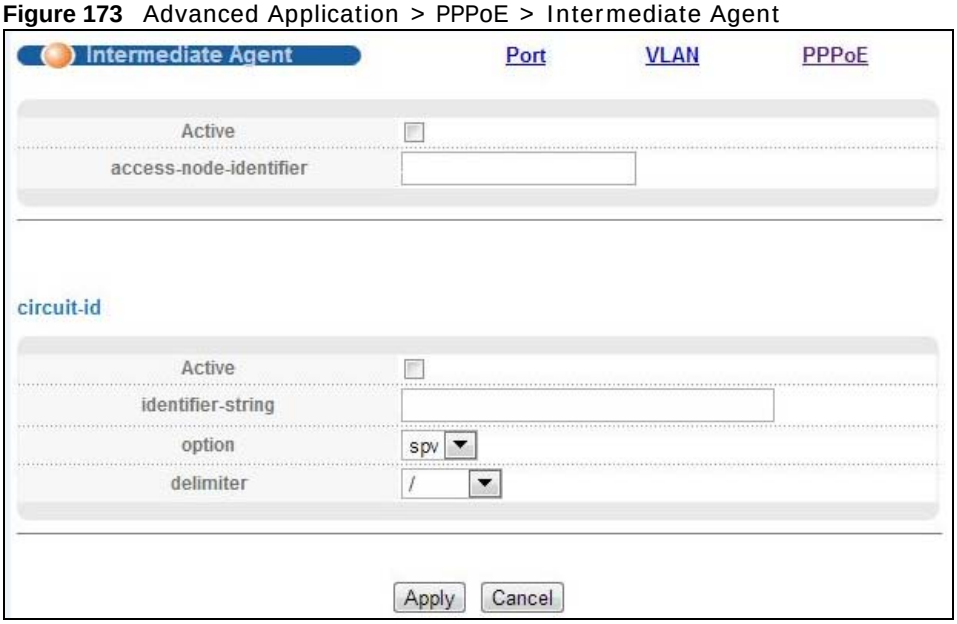


29.3 PPPoE Intermediate Agent

Use this screen to configure the Switch to give a PPPoE termination server additional subscriber information that the server can use to identify and authenticate a PPPoE client.

Click **Advanced Application** > **PPPoE > Intermediate Agent** in the navigation panel to display the screen as shown.

Figure 173 Advanced Application > PPPoE > Intermediate Agent



The following table describes the labels in this screen.

Table 118 Advanced Application > PPPoE > Intermediate Agent

LABEL	DESCRIPTION
Active	Select this option to enable the PPPoE intermediate agent globally on the Switch.
access-node-identifier	Enter up to 20 ASCII characters to identify the PPPoE intermediate agent. Hyphens (-) and spaces are also allowed. The default is the Switch's host name.

Table 118 Advanced Application > PPPoE > Intermediate Agent (continued)

LABEL	DESCRIPTION
circuit-id	Use this section to configure the Circuit ID field in the PADI and PADR packets. The Circuit ID you configure for a specific port or for a specific VLAN on a port has priority over this. The Circuit ID you configure for a specific port (in the **Advanced Application > PPPoE > Intermediate Agent > Port** screen) or for a specific VLAN on a port (in the **Advanced Application > PPPoE > Intermediate Agent > Port > VLAN** screen) has priority over this. That means, if you also want to configure PPPoE IA Per-Port or Per-Port Per-VLAN setting, leave the fields here empty and configure circuit-id and remote-id in the Per-Port or Per-Port Per-VLAN screen.
Active	Select this option to have the Switch add the user-defined identifier string and variables (specified in the **option** field) to PADI or PADR packets from PPPoE clients. If you leave this option unselected, the Switch will use the string specified in the **access-node-identifier** field.
identifier-string	Specify a string that the Switch adds in the Agent Circuit ID sub-option. You can enter up to 53 ASCII characters. Spaces are allowed.
option	Select the variables that you want the Switch to generate and add in the Agent Circuit ID sub-option. The variable options include **sp**, **sv**, **pv** and **spv** which indicate combinations of slot-port, slot-VLAN, port-VLAN and slot-port-VLAN respectively. The Switch enters a zero into the PADI and PADR packets for the slot value.
delimiter	Select a delimiter to separate the identifier-string, slot ID, port number and/or VLAN ID from each other. You can use a pound key (**#**), semi-colon (**;**), period (**.**), comma (**,**), forward slash (**/**) or space.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

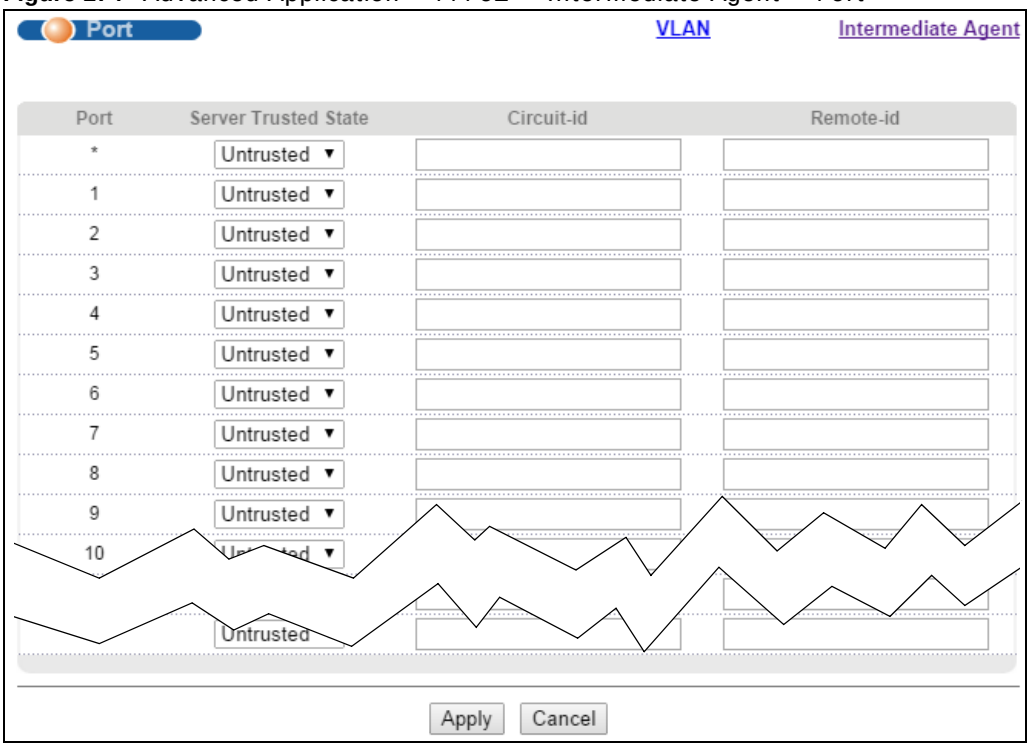
29.3.1 PPPoE IA Per-Port

Use this screen to specify whether individual ports are trusted or untrusted ports and have the Switch add extra information to PPPoE discovery packets from PPPoE clients on a per-port basis.

Note: The Switch will drop all PPPoE packets if you enable the PPPoE Intermediate Agent on the Switch and there are no trusted ports.

Click the **Port** link in the **Intermediate Agent** screen to display the screen as shown.

Figure 174 Advanced Application > PPPoE > Intermediate Agent > Port



The following table describes the labels in this screen.

Table 119 Advanced Application > PPPoE > Intermediate Agent > Port

LABEL	DESCRIPTION
Port	This field displays the port number.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments on a port-by-port basis. Changes in this row are copied to all the ports as soon as you make them.
Server Trusted State	Select whether this port is a trusted port (**Trusted**) or an untrusted port (**Untrusted**). Trusted ports are uplink ports connected to PPPoE servers. If a PADO (PPPoE Active Discovery Offer), PADS (PPPoE Active Discovery Session-confirmation), or PADT (PPPoE Active Discovery Terminate) packet is sent from a PPPoE server and received on a trusted port, the Switch forwards it to all other ports. If a PADI or PADR packet is sent from a PPPoE client but received on a trusted port, the Switch forwards it to other trusted port(s). Untrusted ports are downlink ports connected to subscribers. If a PADI, PADR, or PADT packet is sent from a PPPoE client and received on an untrusted port, the Switch adds a vendor-specific tag to the packet and then forwards it to the trusted port(s). The Switch discards PADO and PADS packets which are sent from a PPPoE server but received on an untrusted port.
Circuit-id	Enter a string of up to 63 ASCII characters that the Switch adds into the Agent Circuit ID sub-option for PPPoE discovery packets received on this port. Spaces are allowed. The Circuit ID you configure for a specific VLAN on a port (in the **Advanced Application > PPPoE > Intermediate Agent > Port > VLAN** screen) has the highest priority.

Table 119 Advanced Application > PPPoE > Intermediate Agent > Port (continued)

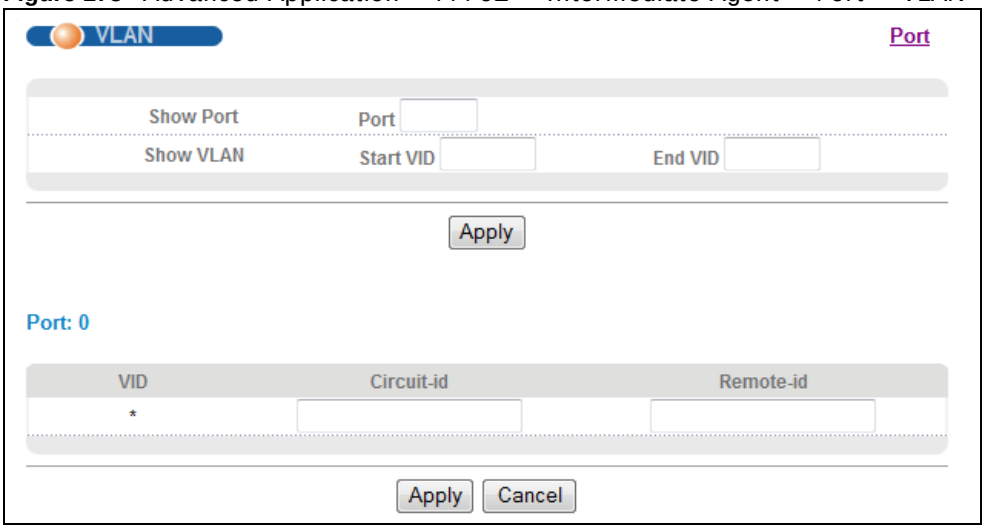
LABEL	DESCRIPTION
Remote-id	Enter a string of up to 63 ASCII characters that the Switch adds into the Agent Remote ID sub-option for PPPoE discovery packets received on this port. Spaces are allowed. If you do not specify a string here or in the **Remote-id** field for a VLAN on a port, the Switch automatically uses the PPPoE client's MAC address. The Remote ID you configure for a specific VLAN on a port (in the **Advanced Application > PPPoE > Intermediate Agent > Port > VLAN** screen) has the highest priority.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

29.3.2 PPPoE IA Per-Port Per-VLAN

Use this screen to configure PPPoE IA settings that apply to a specific VLAN on a port.

Click the **VLAN** link in the **Intermediate Agent > Port** screen to display the screen as shown.

Figure 175 Advanced Application > PPPoE > Intermediate Agent > Port > VLAN



The following table describes the labels in this screen.

Table 120 Advanced Application > PPPoE > Intermediate Agent > Port > VLAN

LABEL	DESCRIPTION
Show Port	Enter a port number to show the PPPoE Intermediate Agent settings for the specified VLAN(s) on the port.
Show VLAN	Use this section to specify the VLANs you want to configure in the section below.
Start VID	Enter the lowest VLAN ID you want to configure in the section below.
End VID	Enter the highest VLAN ID you want to configure in the section below.
Apply	Click **Apply** to display the specified range of VLANs in the section below.
Port	This field displays the port number specified above.
VID	This field displays the VLAN ID of each VLAN in the range specified above. If you configure the ***** VLAN, the settings are applied to all VLANs.

Table 120 Advanced Application > PPPoE > Intermediate Agent > Port > VLAN (continued)

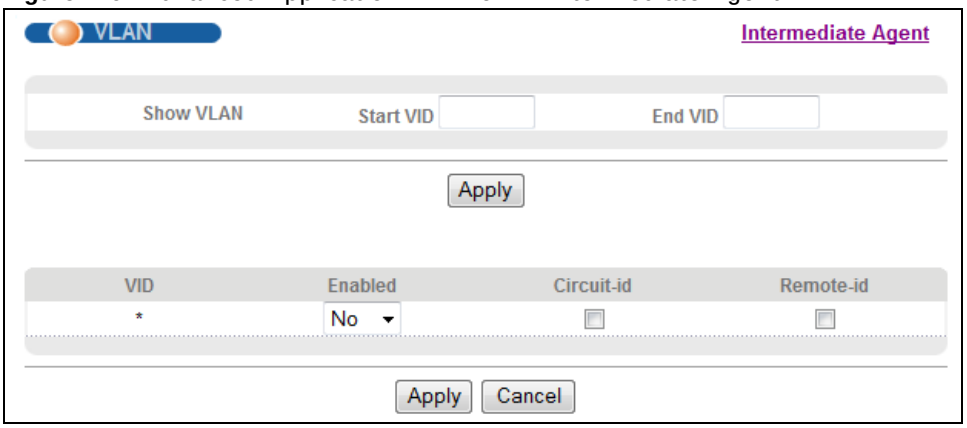
LABEL	DESCRIPTION
*	Use this row to make the setting the same for all VLANs. Use this row first and then make adjustments on a VLAN-by-VLAN basis. Changes in this row are copied to all the VLANs as soon as you make them.
Circuit-id	Enter a string of up to 63 ASCII characters that the Switch adds into the Agent Circuit ID sub-option for this VLAN on the specified port. Spaces are allowed. The Circuit ID you configure here has the highest priority.
Remote-id	Enter a string of up to 63 ASCII characters that the Switch adds into the Agent Remote ID sub-option for this VLAN on the specified port. Spaces are allowed. If you do not specify a string here or in the **Remote-id** field for a specific port, the Switch automatically uses the PPPoE client's MAC address. The Remote ID you configure here has the highest priority.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

29.3.3 PPPoE IA for VLAN

Use this screen to set whether the PPPoE Intermediate Agent is enabled on a VLAN and whether the Switch appends the Circuit ID and/or Remote ID to PPPoE discovery packets from a specific VLAN.

Click the **VLAN** link in the **Intermediate Agent** screen to display the screen as shown.

Figure 176 Advanced Application > PPPoE > Intermediate Agent > VLAN



The following table describes the labels in this screen.

Table 121 Advanced Application > PPPoE > Intermediate Agent > VLAN

LABEL	DESCRIPTION
Show VLAN	Use this section to specify the VLANs you want to configure in the section below.
Start VID	Enter the lowest VLAN ID you want to configure in the section below.
End VID	Enter the highest VLAN ID you want to configure in the section below.
Apply	Click **Apply** to display the specified range of VLANs in the section below.
VID	This field displays the VLAN ID of each VLAN in the range specified above. If you configure the ***** VLAN, the settings are applied to all VLANs.

Table 121 Advanced Application > PPPoE > Intermediate Agent > VLAN (continued)

LABEL	DESCRIPTION
*	Use this row to make the setting the same for all VLANs. Use this row first and then make adjustments on a VLAN-by-VLAN basis. Changes in this row are copied to all the VLANs as soon as you make them.
Enabled	Select this option to turn on the PPPoE Intermediate Agent on a VLAN.
Circuit-id	Select this option to make the Circuit ID settings for a specific VLAN take effect.
Remote-id	Select this option to make the Remote ID settings for a specific VLAN take effect.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

30

Error Disable

30.1 Error Disable Overview

This chapter shows you how to configure the rate limit for control packets on a port, and set the Switch to take an action (such as to shut down a port or stop sending packets) on a port when the Switch detects a pre-configured error. It also shows you how to configure the Switch to automatically undo the action after the error is gone.

30.2 The Error Disable Screens Overview

- Use the **Errdisable Status** screen (Section 30.3 on page 252) to view whether the Switch detected that control packets exceeded the rate limit configured for a port and related information.
- Use the **CPU Protection** screen (Section 30.4 on page 254) to limit the maximum number of control packets (ARP, BPDU and/or IGMP) that the Switch can receive or transmit on a port.
- Use the **Errdisable Detect** screen (Section 30.5 on page 255) to have the Switch detect whether the control packets exceed the rate limit configured for a port and configure the action to take once the limit is exceeded.
- Use the **Errdisable Recovery** screen (Section 30.6 on page 256) to set the Switch to automatically undo an action after the error is gone.

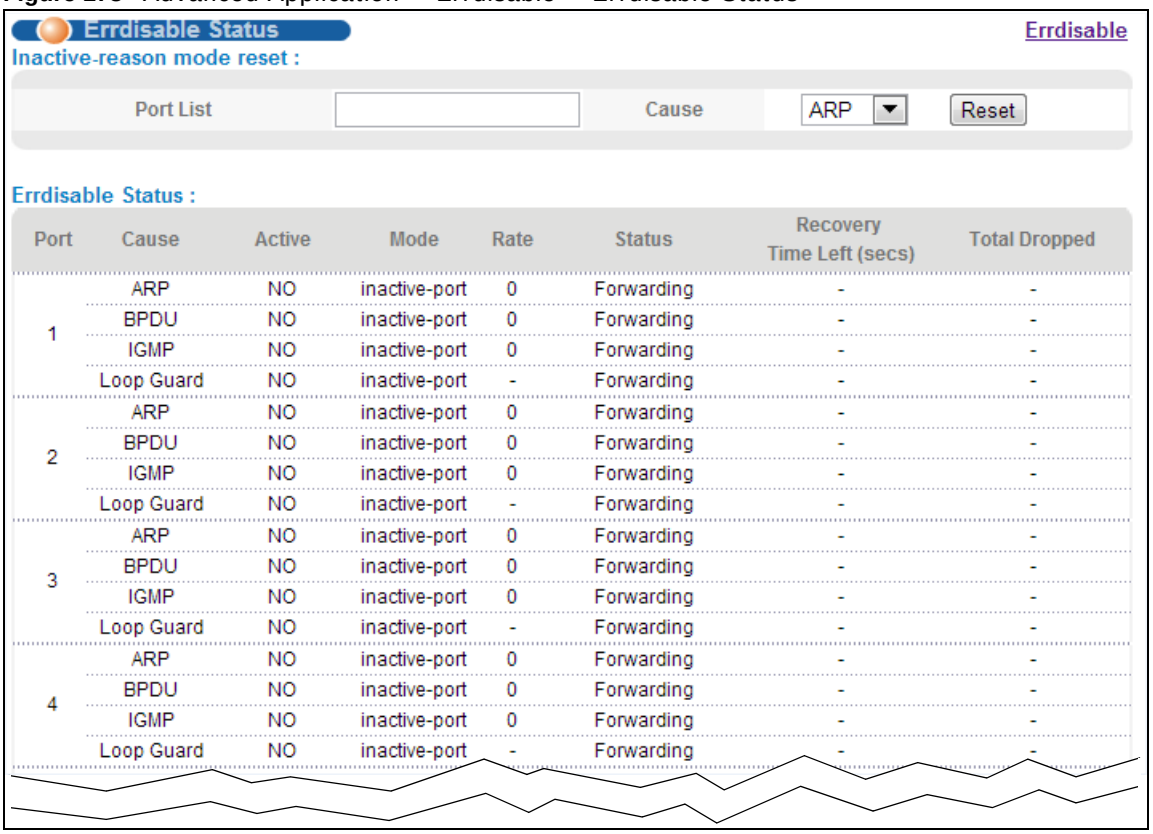
Use this screen to configure error disable related settings. Click **Advanced Application > Errdisable** in the navigation panel to open the following screen.

Figure 177 Advanced Application > Errdisable

30.3 Error-Disable Status

Use this screen to view whether the Switch detected that control packets exceeded the rate limit configured for a port and related information. Click the **Click here** link next to **Errdisable Status** in the **Advanced Application > Errdisable** screen to display the screen as shown.

Figure 178 Advanced Application > Errdisable > Errdisable Status


Errdisable Status
Errdisable
Inactive-reason mode reset :
Port List
Cause
ARP
Reset
Errdisable Status :
Port
Cause
Active
Mode
Rate
Status
Recovery Time Left (secs)
Total Dropped
1 ARP NO inactive-port 0 Forwarding - -
1 BPDU NO inactive-port 0 Forwarding - -
1 IGMP NO inactive-port 0 Forwarding - -
1 Loop Guard NO inactive-port - Forwarding - -
2 ARP NO inactive-port 0 Forwarding - -
2 BPDU NO inactive-port 0 Forwarding - -
2 IGMP NO inactive-port 0 Forwarding - -
2 Loop Guard NO inactive-port - Forwarding - -
3 ARP NO inactive-port 0 Forwarding - -
3 BPDU NO inactive-port 0 Forwarding - -
3 IGMP NO inactive-port 0 Forwarding - -
3 Loop Guard NO inactive-port - Forwarding - -
4 ARP NO inactive-port 0 Forwarding - -
4 BPDU NO inactive-port 0 Forwarding - -
4 IGMP NO inactive-port 0 Forwarding - -
4 Loop Guard NO inactive-port - Forwarding - -

The following table describes the labels in this screen.

Table 122 Advanced Application > Errdisable > Errdisable Status

LABEL	DESCRIPTION
Inactive-reason mode reset	
Port List	Enter the number of the port(s) (separated by a comma) on which you want to reset inactive-reason status.
Cause	Select the cause of inactive-reason mode you want to reset here.
Reset	Press to reset the specified port(s) to handle ARP, BPDU or IGMP packets instead of ignoring them, if the port(s) is in inactive-reason mode.
Errdisable Status	
Port	This is the number of the port on which you want to configure Errdisable Status.
Cause	This refers to the cause of Errdisable Detect or Errdisable Recovery on the Switch.
Active	This field displays whether ARP, BPDU, IGMP and LOOP GUARD on the port is being detected or not.
Mode	This field shows the mode of the cause. • **inactive-port** - The Switch disables the port on which the control packets are received. • **inactive-reason** - The Switch drops all the specified control packets (such as BPDU) on the port. • **rate-limitation** - The Switch drops the additional control packets the port(s) has to handle in every one second.
Rate	This field displays how many control packets this port can receive or transmit per second. It can be adjusted in CPU Protection. **0** means no rate limit.

Table 122 Advanced Application > Errdisable > Errdisable Status (continued)

LABEL	DESCRIPTION
Status	This field displays the errdisable status • **Forwarding**: The Switch is forwarding packets. Rate-limitation mode is always in **Forwarding** status. • **Err-disable**: The Switch disables the port on which the control packets are received (inactive-port) or drops specified control packets on the port (inactive-reason)
Recovery Time	This field displays the time (seconds) left before the port(s) becomes active of Errdisable Recovery.
Total Dropped	This field displays the total packet number dropped by this port where the packet rate exceeds the rate of mode rate-limitation.

30.4 CPU Protection Configuration

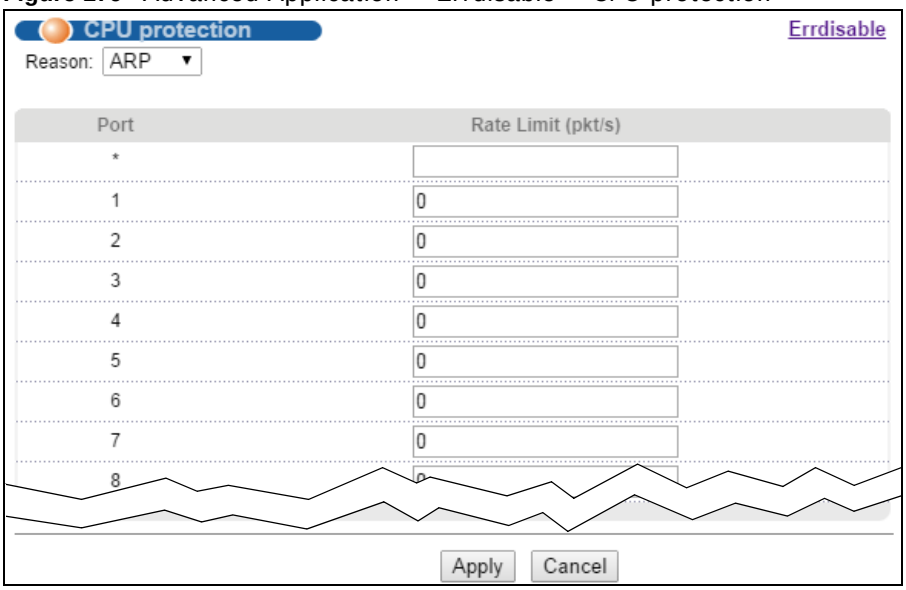
Switches exchange protocol control packets in a network to get the latest networking information. If a switch receives large numbers of control packets, such as ARP, BPDU or IGMP packets, which are to be processed by the CPU, the CPU may become overloaded and be unable to handle regular tasks properly.

The CPU protection feature allows you to limit the rate of ARP, BPDU and IGMP packets to be delivered to the CPU on a port. This enhances the CPU efficiency and protects against potential DoS attacks or errors from other network(s). Then, you can choose to drop or bypass the control packets, decrease the priority value to CPU of control packets that exceed the specified rate limit or disable a port on which the packets are received.

Use this screen to limit the maximum number of control packets (ARP, BPDU and/or IGMP) that the Switch can receive or transmit on a port. Click the **Click Here** link next to **CPU protection** in the **Advanced Application > Errdisable** screen to display the screen as shown.

Note: After you configure this screen, make sure you also enable error detection for the specific control packets in the **Advanced Application** > **Errdisable** > **Errdisable Detect** screen.

Figure 179 Advanced Application > Errdisable > CPU protection



The following table describes the labels in this screen.

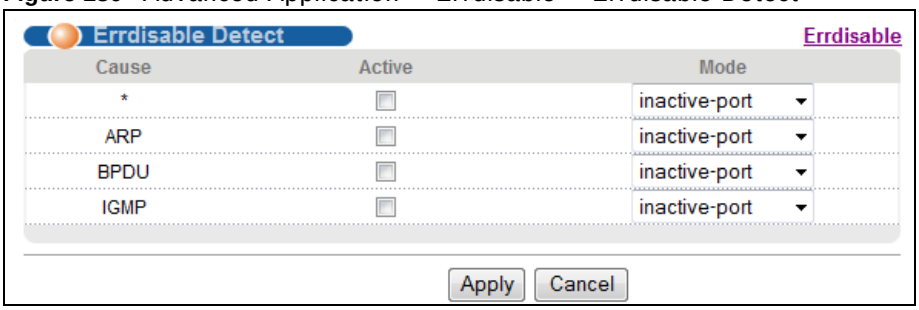
Table 123 Advanced Application > Errdisable > CPU protection

LABEL	DESCRIPTION
Reason	Select the type of control packet you want to configure here.
Port	This field displays the port number.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments to each port if necessary. Changes in this row are copied to all the ports as soon as you make them.
Rate Limit (pkt/s)	Enter a number from 0 to 256 to specify how many control packets this port can receive or transmit per second. **0** means no rate limit. You can configure the action that the Switch takes when the limit is exceeded. See Section 30.5 on page 255 for detailed information.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

30.5 Error-Disable Detect Configuration

Use this screen to have the Switch detect whether the control packets exceed the rate limit configured for a port and configure the action to take once the limit is exceeded. Click the **Click Here** link next to **Errdisable Detect** link in the **Advanced Application > Errdisable** screen to display the screen as shown.

Figure 180 Advanced Application > Errdisable > Errdisable Detect



The following table describes the labels in this screen.

Table 124 Advanced Application > Errdisable > Errdisable Detect

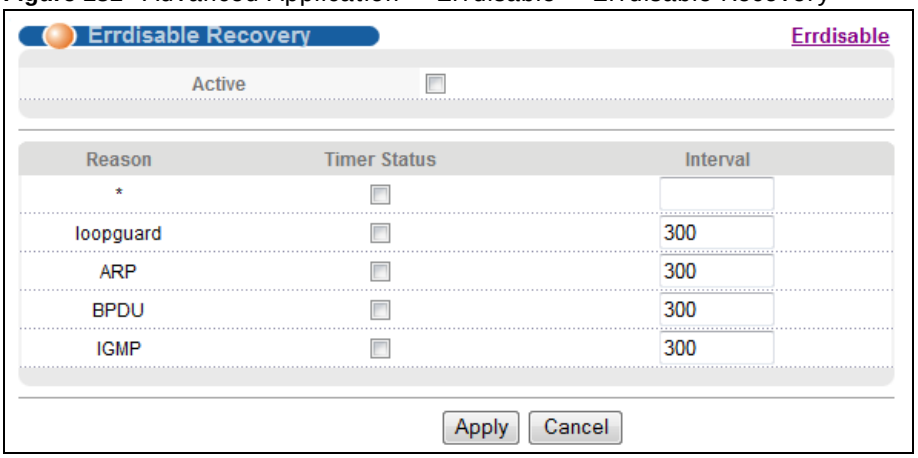
LABEL	DESCRIPTION
Cause	This field displays the types of control packet that may cause CPU overload.
*	Use this row to make the setting the same for all entries. Use this row first and then make adjustments to each entry if necessary. Changes in this row are copied to all the entries as soon as you make them.
Active	Select this option to have the Switch detect if the configured rate limit for a specific control packet is exceeded and take the action selected below.
Mode	Select the action that the Switch takes when the number of control packets exceed the rate limit on a port, set in the **Advanced Application > Errdisable > CPU protection** screen. **inactive-port** - The Switch disables the port on which the control packets are received. **inactive-reason** - The Switch drops all the specified control packets (such as BPDU) on the port. **rate-limitation** - The Switch drops the additional control packets the port has to handle every second.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

30.6 Error-Disable Recovery Configuration

Some features, such as loop guard or CPU protection, allow the Switch to shut down a port or discard specific packets on a port when an error is detected on the port. For example, if the Switch detects that packets sent out the port(s) loop back to the Switch, the Switch can shut down the port(s) automatically. After that, you need to enable the port(s) or allow the packets on a port manually via the web configurator. With error-disable recovery, you can set the disabled port(s) to become active or start receiving the packets again after the time interval you specify.

Use this screen to configure the Switch to automatically undo an action after the error is gone. Click the **Click Here** link next to **Errdisable Recovery** in the **Advanced Application > Errdisable** screen to display the screen as shown.

Figure 181 Advanced Application > Errdisable > Errdisable Recovery



The following table describes the labels in this screen.

Table 125 Advanced Application > Errdisable > Errdisable Recovery

LABEL	DESCRIPTION
Active	Select this option to turn on the error-disable recovery function on the Switch.
Reason	This field displays the supported features that allow the Switch to shut down a port or discard packets on a port according to the feature requirements and what action you configure.
*	Use this row to make the setting the same for all entries. Use this row first and then make adjustments to each entry if necessary. Changes in this row are copied to all the entries as soon as you make them.
Timer Status	Select this option to allow the Switch to wait for the specified time interval to activate a port or allow specific packets on a port, after the error was gone. Deselect this option to turn off this rule.
Interval	Enter the number of seconds (from 30 to 2592000) for the time interval.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

31

MAC Pinning

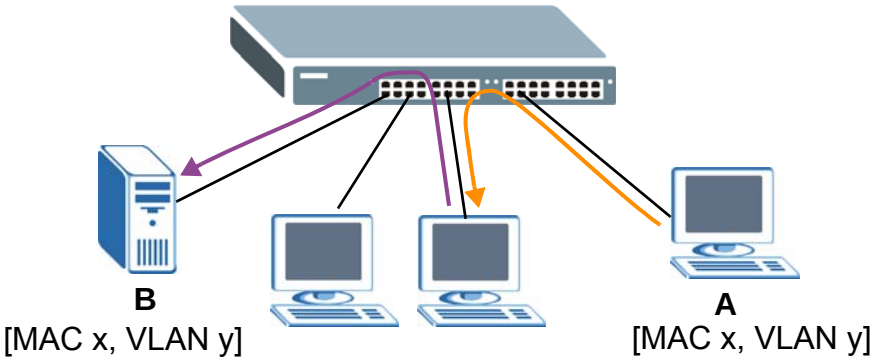
This chapter shows you how to configure MAC pinning on the Switch.

31.1 MAC Pinning Overview

When the Switch obtains a connected device's MAC address, it adds an entry in the MAC address forwarding table and uses the table to determine how to forward frames. In addition to the source MAC address of a received frame, the Switch also learns the VLAN to which the device belongs and the port on which the frame is received. If the Switch learns the same MAC address and same VLAN ID on another port, it updates the MAC address table immediately.

MAC pinning allows you to set a port or multiple ports to have priority over other ports in MAC address learning. That means when a MAC address (and VLAN ID) is learned on a MAC-pinning-enabled port, the MAC address will not be learned on any other port until the aging time for the dynamically learned MAC address in the table expires.

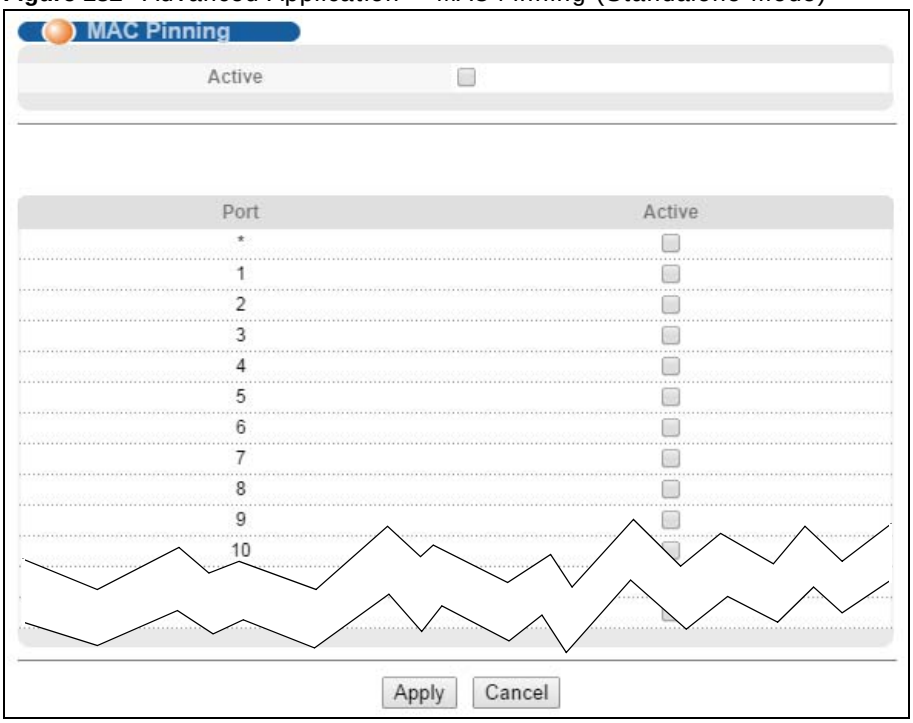
This helps enhance security. For example, when an attacker (**A**) sends packets to all connected clients by spoofing the source MAC address of a server (**B**) connected to one of the Switch's ports, on which MAC pinning is enabled, the responses from clients will still be forwarded to the server according to the Switch's MAC forwarding table.



31.2 MAC Pinning Configuration

Use this screen to enable MAC pinning on the Switch and on specific ports. Click **Advanced Application > MAC Pinning** in the navigation panel to open the following screen.

Figure 182 Advanced Application > MAC Pinning (Standalone mode)



The following table describes the labels in this screen.

Table 126 Advanced Application > MAC Pinning

LABEL	DESCRIPTION
Active	Select this option to turn on the MAC pinning function on the Switch.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments to each port if necessary. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to enable MAC pinning on this port. The port then has priority over other ports in MAC address learning. Clear this check box to disable MAC pinning.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

32

Private VLAN

32.1 Private VLAN Overview

Use private VLAN if you want you to block traffic between ports in the same VLAN. **Community** and **Isolated** VLANs are secondary private VLANs that must be associated with a **Primary** private VLAN.

- **Primary**: Ports in a **Primary** VLAN are promiscuous and they can communicate with all promiscuous ports in the same primary VLAN, and all ports in associated community and isolated VLANs. They cannot communicate with ports in different primary VLANs.
- **Community**: Ports in a **Community** VLAN can communicate with promiscuous ports in an associated **Primary** VLAN and other community ports in the same **Community** VLAN. They cannot communicate with ports in **Isolated** VLANs, non-associated **Primary** VLAN promiscuous ports nor community ports in different **Community** VLANs.
- **Isolated**: Ports in an **Isolated** VLAN can communicate with promiscuous ports in an associated **Primary** VLAN only. They cannot communicate with other isolated ports in the same **Isolated** VLAN, non-associated **Primary** VLAN promiscuous ports nor any community ports.

Figure 183 Private VLAN Overview

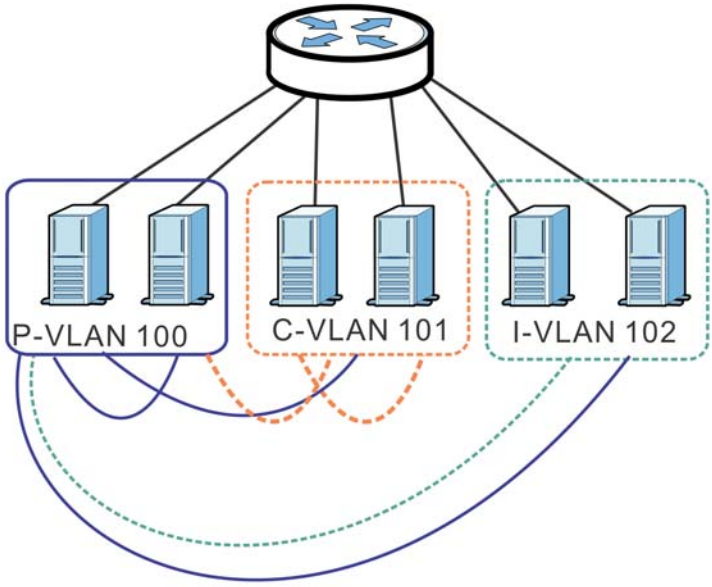


Table 127 PVLAN Graphic Key

LABEL	DESCRIPTION
P-VLAN 100	Primary private VLAN
C-VLAN 101	Community private VLAN
I-VLAN 102	Isolated private VLAN

Tagged Private VLANs can span switches but trunking ports must be VLAN-trunking ports - see **Advanced > VLAN > VLAN Port Setting**.

Figure 184 Private VLAN Spanning Switches

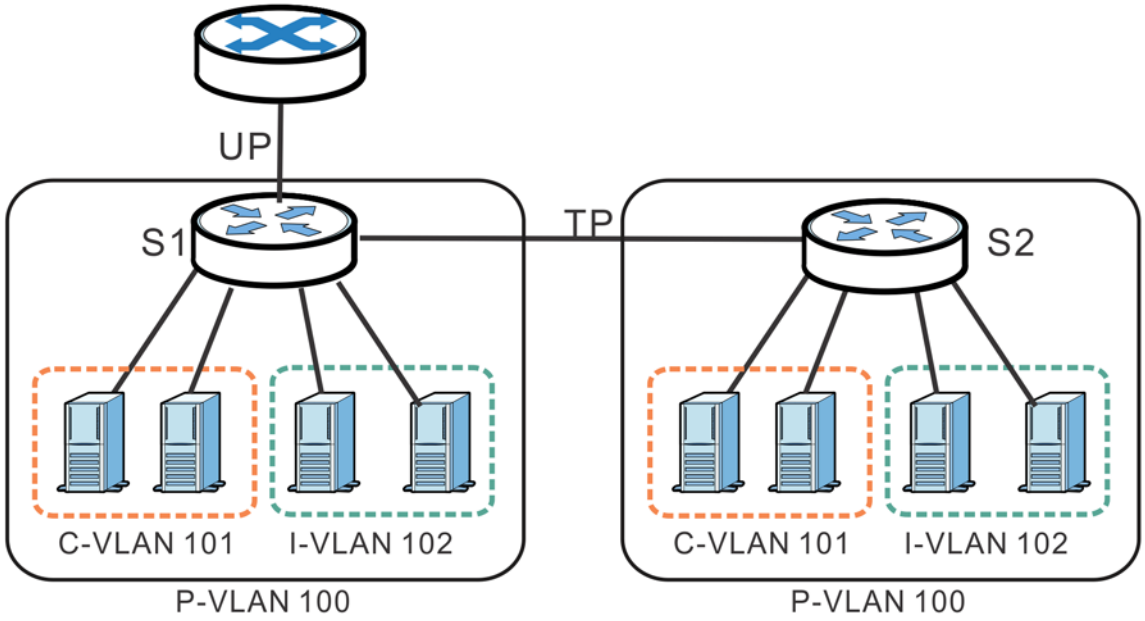


Table 128 Spanning PVLAN Graphic Key

LABEL	DESCRIPTION
UP	Uplink promiscuous port
TP	VLAN-trunking ports
S1, S2	Switch 1, Switch 2
P-VLAN 100	Primary private VLAN with VLAN ID tag of 100
C-VLAN 101	Community private VLAN with VLAN ID tag of 101
I-VLAN 102	Isolated private VLAN with VLAN ID tag of 102

This is the communication process if primary VLAN **P-VLAN 100** is associated with community VLAN **C-VLAN 101** and isolated VLAN **I-VLAN 102**.

- Promiscuous ports in **P-VLAN 100** can communicate with all ports in **P-VLAN 100** including community ports in **C-VLAN 101** and isolated ports in **I-VLAN 102**.

- Community ports in **C-VLAN 101** can communicate with promiscuous ports in **P-VLAN 100** and other community ports in **C-VLAN 101**. They cannot communicate with isolated ports in **I-VLAN 102**.
- Isolated ports can communicate with promiscuous ports in **P-VLAN 100**. They cannot communicate with other isolated ports in **I-VLAN 102** nor community ports in **C-VLAN 101**.

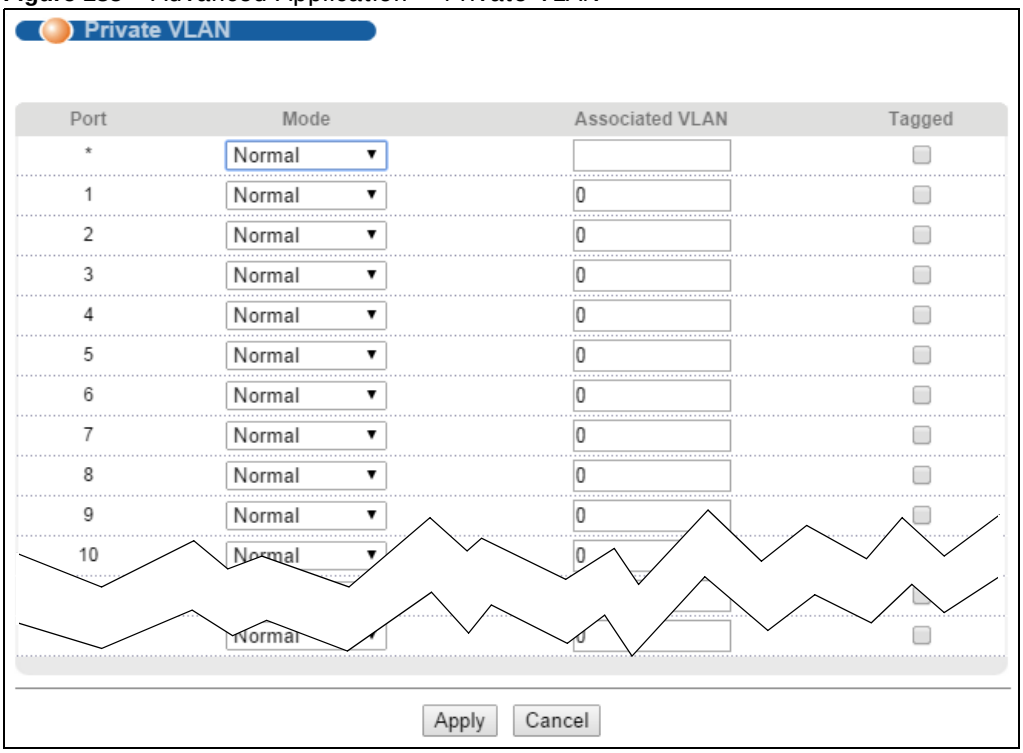
Note: **Isolation** in **VLAN > VLAN Configuration > VLAN Port Setting** (see Section 9.6 on page 94) has a higher priority than private VLAN settings, so promiscuous ports with **Isolation** in **VLAN > VLAN Port Setting** enabled will not be able to communicate with each other.

32.1.1 Configuration

You must go to the **Static VLAN** screen first (see Section 9.5 on page 92) to create VLAN IDs for **Primary**, **Isolated** or **Community** VLANs.

Click **Advanced Application > Private VLAN** to display the following screen.

Figure 185 Advanced Application > Private VLAN



The following table describes the labels in this screen.

Table 129 Advanced Application > Private VLAN

LABEL	DESCRIPTION
Mode	This is the type of VLAN mapped to this port. • **Normal**: These are ports in a static VLAN. This is not a private VLAN. • **Promiscuous**: Ports in a **Primary** VLAN are **Promiscuous**. They can communicate with all ports in the **Primary** VLAN and associated **Community** and **Isolated** VLANs. They cannot communicate with **Promiscuous** ports in different primary VLANs. • **Community**: Ports in a **Community** VLAN can communicate with **Promiscuous** ports in an associated Primary VLAN and other community ports in the same **Community** VLAN. They cannot communicate with ports in an **Isolated** VLAN, non-associated **Primary** VLAN **Promiscuous** ports nor **Community** ports in different **Community** VLANs. • **Isolated:** Ports in an **Isolated** VLAN can communicate with **Promiscuous** ports in an associated **Primary** VLAN only. They cannot communicate with other **Isolated** ports in the same **Isolated** VLAN, non-associated **Primary** VLAN **Promiscuous** ports nor any **Community** ports.
Associated VLAN	Enter the VLAN ID of a previously created VLAN here. Note: The VLAN ID and **Mode** selected here must be the same as the VLAN ID and **VLAN Type** created in **Advanced Application > VLAN > Static VLAN**.
Tagged	A VLAN ID tag identifies VLAN membership of a frame across switches. Select this if the VLAN includes ports on multiple switches. The Switch forwards tagged frames through this port; it adds the PVID to untagged frames before sending them out. Clear this if the VLAN includes ports on this Switch only. The Switch forwards untagged frames through this port; it removes the VLAN ID from tagged frames before sending them out.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

33

Green Ethernet

This chapter shows you how to configure the Switch to reduce the power consumed by switch ports.

33.1 Green Ethernet Overview

Green Ethernet reduces switch port power consumption in the following ways.

IEEE 802.3az Energy Efficient Ethernet (EEE)

If EEE is enabled, both sides of a link support EEE and there is no traffic, the port enters Low Power Idle (LPI) mode. LPI mode turns off some functions of the physical layer (becomes quiet) to save power. Periodically the port transmits a REFRESH signal to allow the link partner to keep the link alive. When there is traffic to be sent, a WAKE signal is sent to the link partner to return the link to active mode.

Auto Power Down

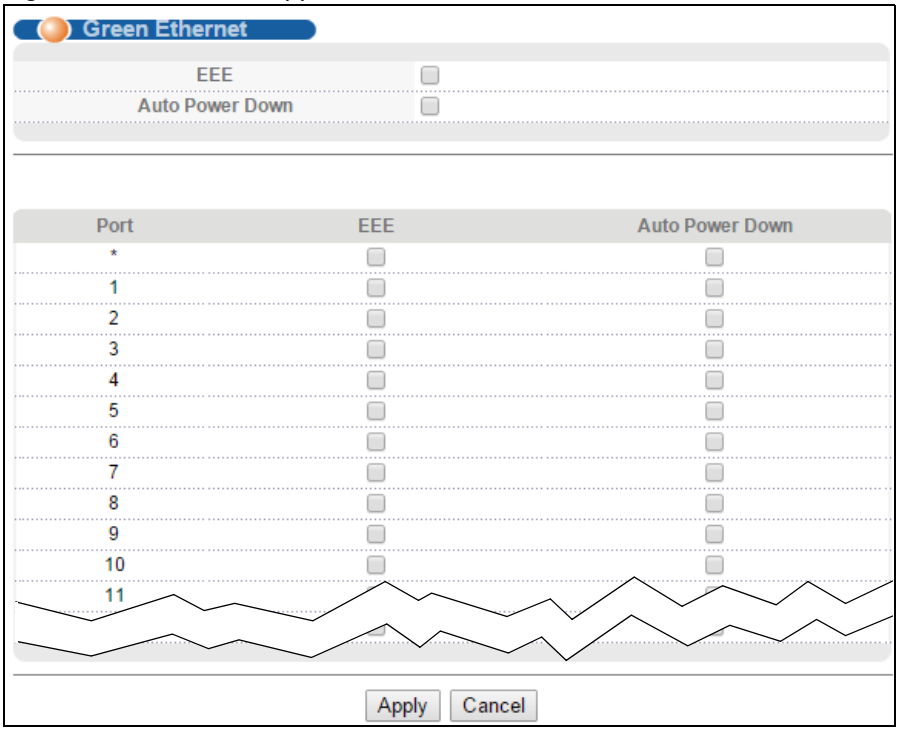
Auto Power Down turns off almost all functions of the port's physical layer functions when the link is down, so the port only uses power to check for a link up pulse from the link partner. After the link up pulse is detected, the port wakes up from **Auto Power Down** and operates normally.

33.2 Configuring Green Ethernet

Click **Advanced Application** > **Green Ethernet** in the navigation panel to display the screen as shown.

Note: EEE and Auto Power Down are not supported on an uplink port.

Figure 186 Advanced Application > Green Ethernet



The following table describes the labels in this screen.

Table 130 Advanced Application > Green Ethernet

LABEL	DESCRIPTION
EEE	Select this to activate Energy Efficient Ethernet globally.
Auto Power Down	Select this to activate Auto Power Down globally.
Port	This field displays the port number.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments to each port if necessary. Changes in this row are copied to all the ports as soon as you make them.
EEE	Select this to activate Energy Efficient Ethernet on this port.
Auto Power Down	Select this to activate Auto Power Down on this port.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

34

Link Layer Discovery Protocol (LLDP)

34.1 LLDP Overview

The LLDP (Link Layer Discovery Protocol) is a layer 2 protocol. It allows a network device to advertise its identity and capabilities on the local network. It also allows the device to maintain and store information from adjacent devices which are directly connected to the network device. This helps an administrator discover network changes and perform necessary network reconfiguration and management. The device information is encapsulated in the LLDPDUs (LLDP data units) in the form of TLV (Type, Length, Value). Device information carried in the received LLDPDUs is stored in the standard MIB.

The Switch supports these basic management TLVs.

- End of LLDPDU (mandatory)
- Chassis ID (mandatory)
- Port ID (mandatory)
- Time to Live (mandatory)
- Port Description (optional)
- System Name (optional)
- System Description (optional)
- System Capabilities (optional)
- Management Address (optional)

The Switch also supports the IEEE 802.1 and IEEE 802.3 organizationally-specific TLVs.

IEEE 802.1 specific TLVs:

- Port VLAN ID TLV (optional)
- Port and Protocol VLAN ID TLV (optional)

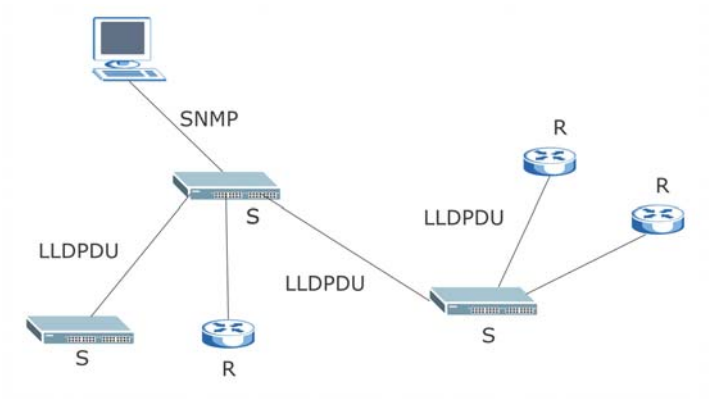
IEEE 802.3 specific TLVs:

- MAC/PHY Configuration/Status TLV (optional)
- Power via MDI TLV (optional, For PoE models only)
- Link Aggregation TLV (optional)
- Maximum Frame Size TLV (optional)

The optional TLVs are inserted between the Time To Live TLV and the End of LLDPDU TLV.

The next figure demonstrates that the network devices Switches and Routers (S and R) transmit and receive device information via LLDPDU and the network manager can query the information using Simple Network Management Protocol (SNMP).

Figure 187 LLDP Overview



34.2 LLDP-MED Overview

LLDP-MED (Link Layer Discovery Protocol for Media Endpoint Devices) is an extension to the standard LLDP developed by the Telecommunications Industry Association (TIA) TR-41.4 subcommittee which defines the enhanced discovery capabilities, such as VoIP applications, to enable network administrators manage their network topology application more efficiently. Unlike the traditional LLDP, which has some limitations when handling multiple application devices, the LLDP-MED offers display of accurate physical topology, interoperability of devices, and easy trouble shooting for misconfigured IP addresses. There are three classes of endpoint devices that the LLDP-MED supports:

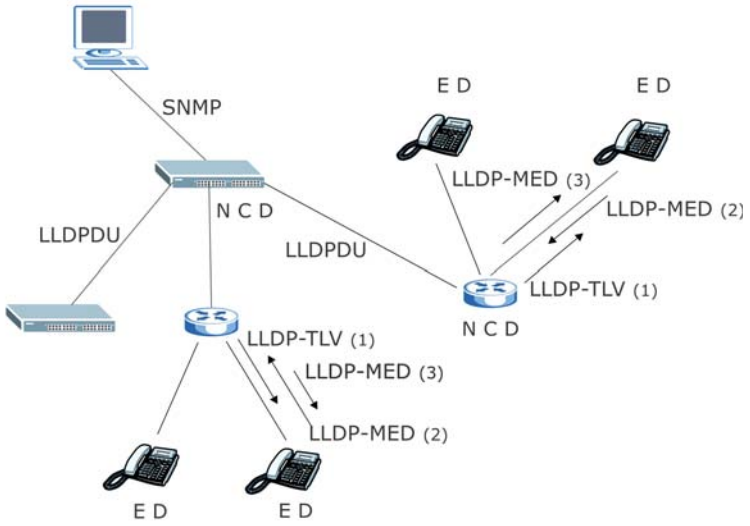
Class I: IP Communications Controllers or other communication related servers

Class II: Voice Gateways, Conference Bridges or Media Servers

Class III: IP-Phones, PC-based Softphones, End user Communication Appliances supporting IP Media

The following figure shows that with the LLDP-MED, network connectivity devices (NCD) like Switches and Routers will transmit LLDP TLV to endpoint device (ED) like IP Phone first (1), to get its device type and capabilities information, then it will receive that information in LLDP-MED TLV back from endpoint devices (2), after that the network connectivity devices will transmit LLDP-MED TLV (3) to provision the endpoint device to such that the endpoint device's network policy and location identification information is updated. Since LLDPDU updates status and configuration information periodically, network managers may check the result of provision via remote status. The remote status is updated by receiving LLDP-MED TLVs from endpoint devices.

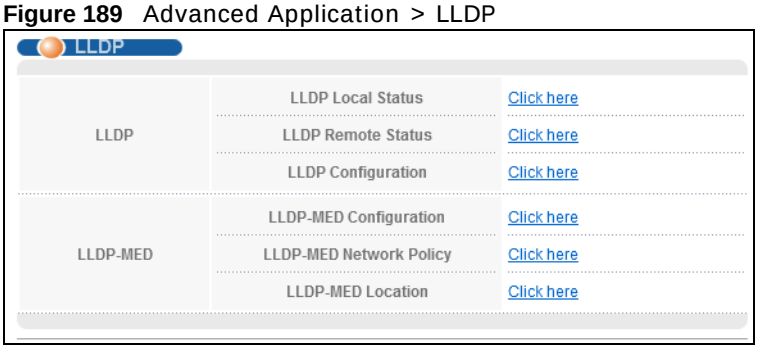
Figure 188 LLDP-MED Overview



34.3 LLDP Screens

Click **Advanced Application** > **LLDP** in the navigation panel to display the screen as shown next.

Figure 189 Advanced Application > LLDP



The following table describes the labels in this screen.

Table 131 Advanced Application > LLDP

LABEL	DESCRIPTION
LLDP	
LLDP Local Status	Click here to show a screen with the Switch's LLDP information.
LLDP Remote Status	Click here to show a screen with LLDP information from the neighboring devices.
LLDP Configuration	Click here to show a screen to configure LLDP parameters.
LLDP-MED	
LLDP-MED Configuration	Click here to show a screen to configure LLDP-MED (Link Layer Discovery Protocol for Media Endpoint Devices) parameters.

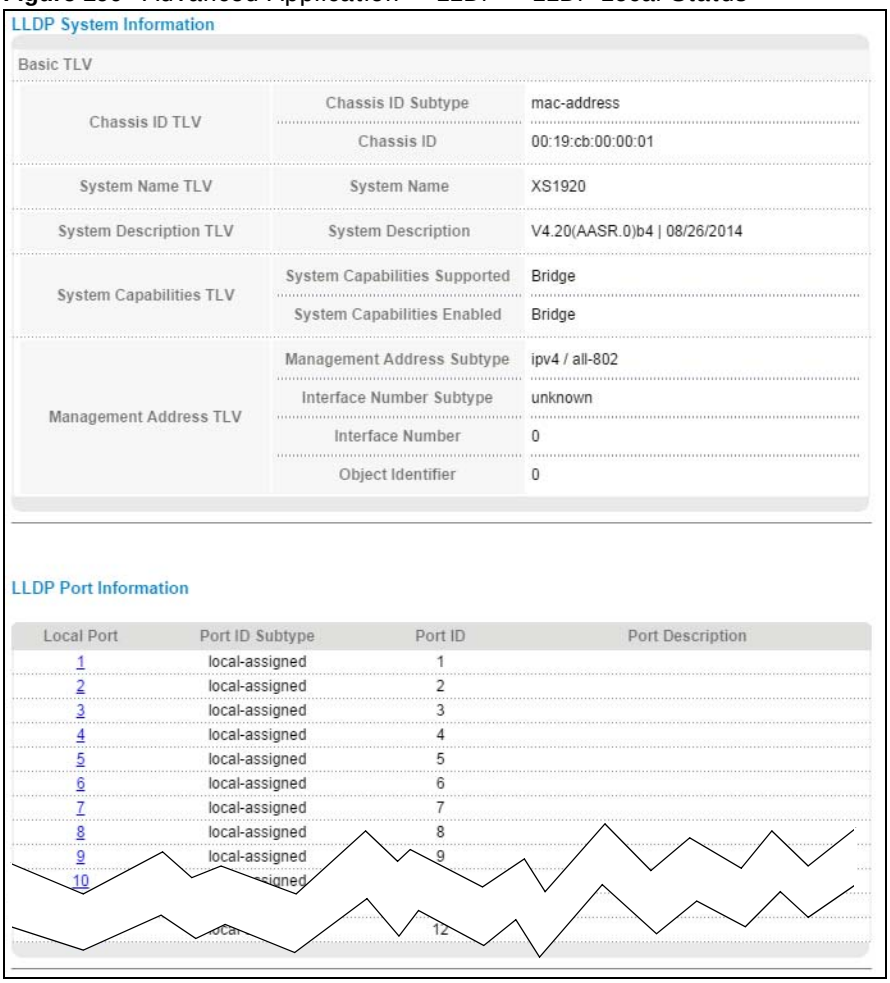
Table 131 Advanced Application > LLDP (continued)

LABEL	DESCRIPTION
LLDP-MED Network Policy	Click here to show a screen to configure LLDP-MED (Link Layer Discovery Protocol for Media Endpoint Devices) network policy parameters.
LLDP-MED Location	Click here to show a screen to configure LLDP-MED (Link Layer Discovery Protocol for Media Endpoint Devices) location parameters.

34.4 LLDP Local Status

This screen displays a summary of LLDP status on this Switch. Click **Advanced Application** > **LLDP > LLDP Local Status (Click Here)** to display the screen as shown next.

Figure 190 Advanced Application > LLDP > LLDP Local Status



The following table describes the labels in this screen.

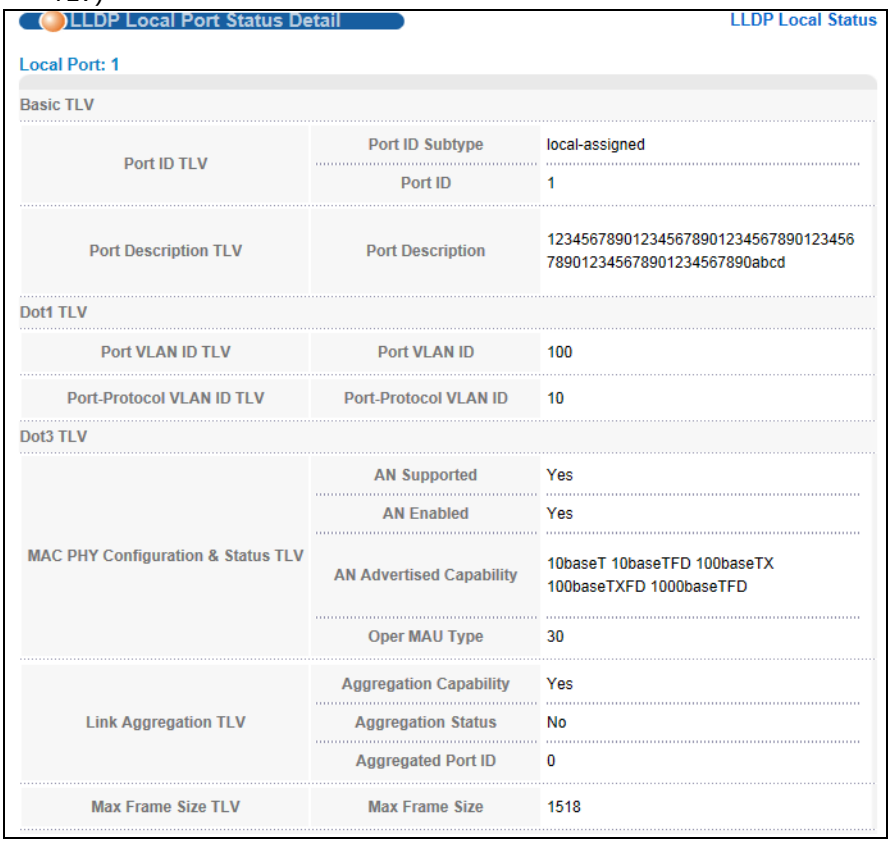
Table 132 Advanced Application > LLDP > LLDP Local Status

LABEL	DESCRIPTION
Basic TLV	
Chassis ID TLV	This displays the chassis ID of the local Switch, that is the Switch you're configuring. The chassis ID is identified by the chassis ID subtype. Chassis ID Subtype - this displays how the chassis of the remote Switch is identified. Chassis ID - This displays the chassis ID of the local Switch. The chassis ID is identified by the chassis ID subtype.
System Name TLV	This shows the Host Name of the Switch.
System Description TLV	This shows the System Description which is the firmware version of the Switch.
System Capabilities TLV	This shows the System Capabilities enabled and supported on the local Switch. • System Capabilities Supported - Bridge • System Capabilities Enabled - Bridge
Management Address TLV	The Management Address TLV identifies an address associated with the local LLDP agent that may be used to reach higher layer entities to assist discovery by network management. The TLV may also include the system interface number and an object identifier (OID) that are associated with this management address This field displays the Management Address settings on the specified port(s). • Management Address Subtype - ipv4 / all-802 • Interface Number Subtype - unknown • Interface Number - 0 (not supported) • Object Number - 0 (not supported)
LLDP Port Information	This displays the local port information.
Local Port	This displays the local port number which receives the LLDPDU from the remote device. Click a port number to view the detailed LLDP status on this port at **LLDP Local Port Status Detail** screen.
Port ID Subtype	This indicates how the port ID field is identified.
Port ID	This is an alpha-numeric string that contains the specific identifier for the port from which this LLDPDU was transmitted.
Port Description	This shows the port description that the Switch will advertise from this port.

34.4.1 LLDP Local Port Status Detail

This screen displays detailed LLDP status for each port on this Switch. Click **Advanced Application** > **LLDP > LLDP Local Status** and then, click a port number, for example 1 (Port) in the local port column to display the screen as shown next.

Figure 191 Advanced Application > LLDP > LLDP Local Status > LLDP Local Port Status Detail (Basic TLV)


LLDP Local Port Status Detail

LLDP Local Status

Local Port: 1

Basic TLV		
Port ID TLV	Port ID Subtype	local-assigned
	Port ID	1
Port Description TLV	Port Description	12345678901234567890123456789012345678901234567890123456789abcd
Dot1 TLV		
Port VLAN ID TLV	Port VLAN ID	100
Port-Protocol VLAN ID TLV	Port-Protocol VLAN ID	10
Dot3 TLV		
MAC PHY Configuration & Status TLV	AN Supported	Yes
	AN Enabled	Yes
	AN Advertised Capability	10baseT 10baseTFD 100baseTX 100baseTXFD 1000baseTFD
	Oper MAU Type	30
Link Aggregation TLV	Aggregation Capability	Yes
	Aggregation Status	No
	Aggregated Port ID	0
Max Frame Size TLV	Max Frame Size	1518

Figure 192 Advanced Application > LLDP > LLDP Local Status > LLDP Local Port Status Detail (MED TLV)

MED TLV

Capabilities TLV	Network Policy	Yes
	Location	Yes
	Extend Power via MDI PSE	No
	Extend Power via MDI PD	No
	Inventory Management	No
Device Type TLV	Device Type	Network Connectivity
Network Policy TLV	Voice	VLAN ID 10, tagged, L2-priority 7, DSCP 63
	Voice-Signaling	VLAN ID 100, tagged, L2-priority 2, DSCP 10
	Guest-Voice	VLAN ID 20, tagged, L2-priority 3, DSCP 12
	Guest-Voice-Signaling	VLAN ID 0, untagged, L2-priority 0, DSCP 0
	Softphone-Voice	VLAN ID 200, tagged, L2-priority 1, DSCP 1
	Video-Conferencing	VLAN ID 0, untagged, L2-priority 0, DSCP 0
	Streaming-Video	VLAN ID 300, tagged, L2-priority 4, DSCP 20
	Video-Signaling	VLAN ID 400, tagged, L2-priority 6, DSCP 55
Location Identification TLV	Coordinate-base LCI	latitute north 24.0 longitute east 120.0 altitute meter 13.0 datum WGS84
	Civic LCI	country TW city HSINCHU building ZYXEL
	ELIN	1234567890

The following table describes the labels in this screen.

Table 133 Advanced Application > LLDP > LLDP Local Status > LLDP Local Port Status Detail

LABEL	DESCRIPTION
Basic TLV	These are the Basic TLV flags
Port ID TLV	The port ID TLV identifies the specific port that transmitted the LLDP frame. • Port ID Subtype: This shows how the port is identified. • Port ID: This is the ID of the port.
Port Description TLV	This displays the local port description.
Dot1 TLV	
Port VLAN ID TLV	This displays the VLAN ID sent by the IEEE 802.1 Port VLAN ID TLV.
Port-Protocol VLAN ID TLV	This displays the IEEE 802.1 Port Protocol VLAN ID TLVs, which indicates whether the VLAN is enabled and supported.
Dot3 TLV	
MAC PHY Configuration & Status TLV	The MAC/PHY Configuration/Status TLV advertises the bit-rate and duplex capability of the sending 802.3 node. It also advertises the current duplex and bit-rating of the sending node. Lastly, it advertises whether these setting were the result of auto-negotiation during link initiation or manual override. • AN Supported - Displays if the port supports or does not support auto-negotiation. • AN Enabled - The current auto-negotiation status of the port. • AN Advertised Capability - The auto-negotiation capabilities of the port. • Oper MAU Type - The current Medium Attachment Unit (MAU) type of the port
Link Aggregation TLV	The Link Aggregation TLV indicates whether the link is capable of being aggregated, whether the link is currently in an aggregation, and if in an aggregation, the port identification of the aggregation. • Aggregation Capability — The current aggregation capability of the port. • Aggregation Status — The current aggregation status of the port. • Aggregation Port ID — The aggregation ID of the current port.
Max Frame Size TLV	This displays the maximum supported frame size in octets.
MED TLV	LLDP Media Endpoint Discovery (MED) is an extension of LLDP that provides additional capabilities to support media endpoint devices. MED enables advertisement and discovery of network policies, device location discovery to allow creation of location databases, and information for troubleshooting.
Capabilities TLV	This field displays which LLDP-MED TLV are capable to transmit on the Switch. • Network Policy • Location
Device Type TLV	This is the LLDP-MED device class. The Zyxel Switch device type is: • Network Connectivity

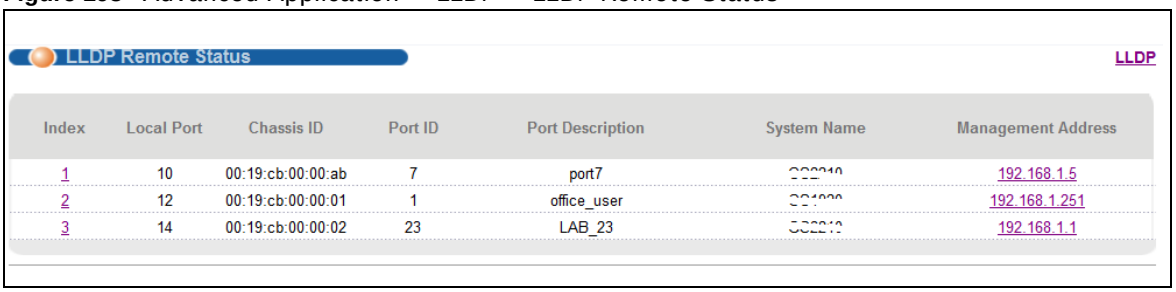
Table 133 Advanced Application > LLDP > LLDP Local Status > LLDP Local Port Status Detail

LABEL	DESCRIPTION
Network Policy TLV	This displays a network policy for the specified application. • Voice • Voice-Signaling • Guest-Voice • Guest-Voice-Signaling • Softphone-Voice • Video-Conferencing • Streaming-Video • Video-Signaling
Location Identification TLV	This shows the location information of a caller by its ELIN (Emergency Location Identifier Number) or the IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI). • Civic LCI - IETF Geopriv Civic Address based Location Configuration Information • ELIN - (Emergency Location Identifier Number) • Coordinate-based LCI - latitude, longitude and altitude coordinates of the location Configuration Information (LCI)

34.5 LLDP Remote Status

This screen displays a summary of LLDP status for each LLDP connection to a neighboring Switch. Click **Advanced Application** > **LLDP > LLDP Remote Status (Click Here)** to display the screen as shown next.

Figure 193 Advanced Application > LLDP > LLDP Remote Status



The following table describes the labels in this screen.

Table 134 Advanced Application > LLDP > LLDP Remote Status

LABEL	DESCRIPTION
Index	The index number shows the number of remote devices that are connected to the Switch. Click on an index number to view the detailed LLDP status for this remote device at **LLDP Remote Port Status Detail** screen.
Local Port	This is the port number of local Switch that recieved LLDPDU from the remote device.
Chassis ID	This displays the chassis ID of the remote device associated with the transmitting LLDP agent. The chassis ID is identified by the chassis ID subtype. For example, the MAC address of the remote device.
Port ID	This is an alpha-numeric string that contains the specific identifier for the port from which this LLDPDU was transmitted. The port ID is identified by the port ID subtype.
Port Description	This displays a description for the port from which this LLDPDU was transmitted.

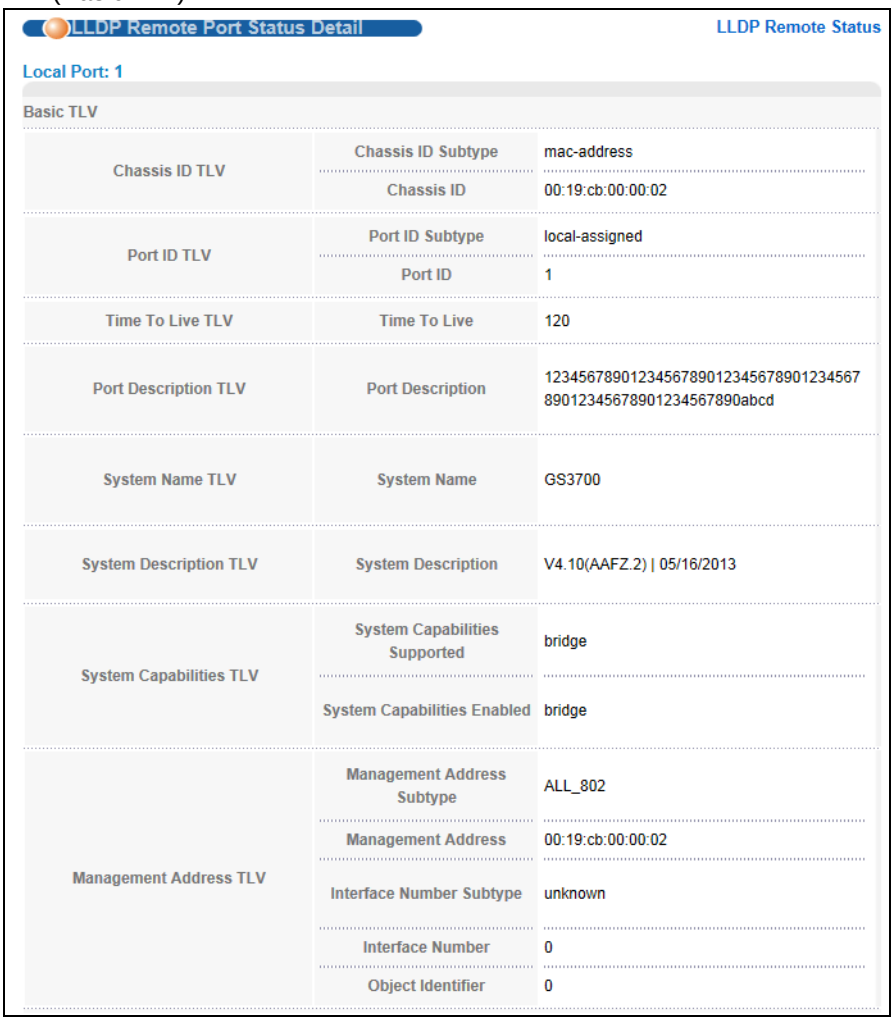
Table 134 Advanced Application > LLDP > LLDP Remote Status

LABEL	DESCRIPTION
System Name	This displays the system name of the remote device.
Management Address	This displays the management address of the remote device. It could be the MAC address or IP address. You can click on the IP address hyperlink directly.

34.5.1 LLDP Remote Port Status Detail

This screen displays detailed LLDP status received from remote device. Click **Advanced Application** > **LLDP > LLDP Remote Status (Click Here)** and then click an index number, for example 1, in the Index column in the **LLDP Remote Status** screen to display the screen as shown next.

Figure 194 Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail (Basic TLV)

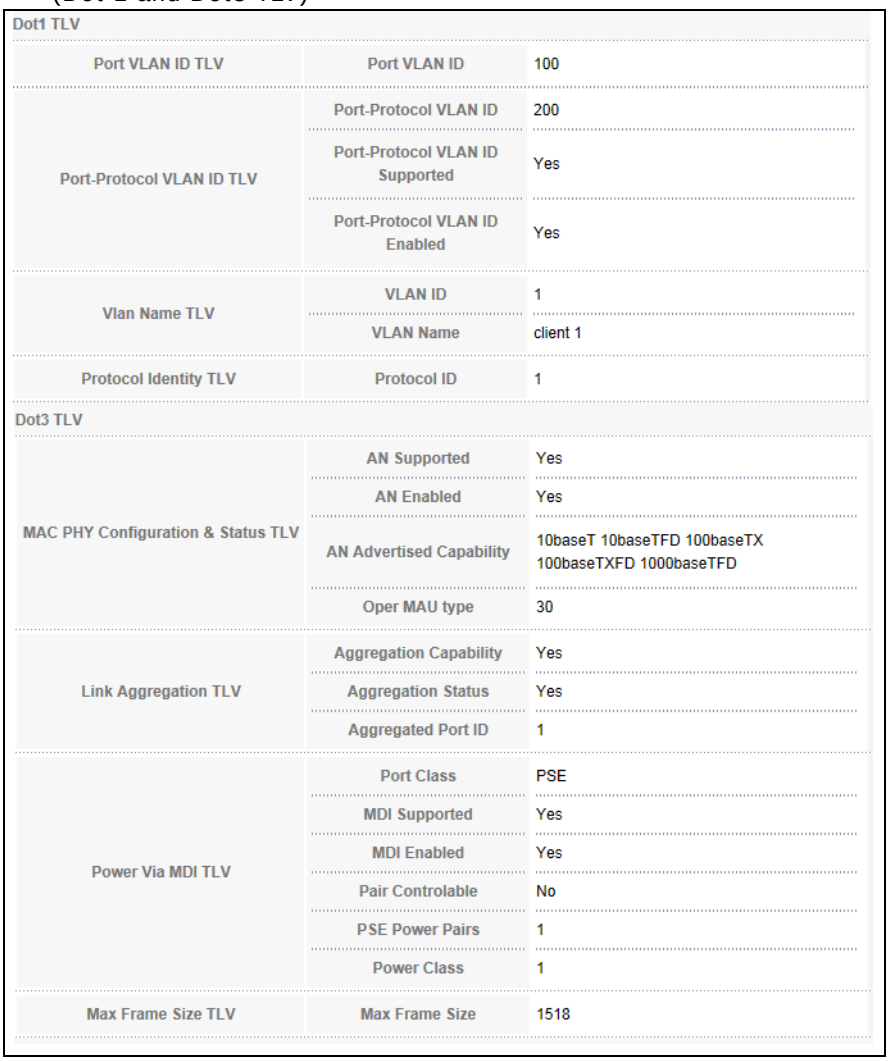


The following table describes the labels in Basic TLV part of the screen.

Table 135 Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail (Basic TLV)

LABEL	DESCRIPTION
Basic TLV	
Chassis ID TLV	• Chassis ID Subtype - this displays how the chassis of the remote device is identified. • Chassis ID - this displays the chassis ID of the remote device. The chassis ID is identified by the chassis ID subtype
Port ID TLV	• Port ID Subtype - this displays how the port of the remote device is identified. • Port ID - this displays the port ID of the remote device. The port ID is identified by the port ID subtype.
Time To Live TLV	This displays the time-to-live (TTL) multiplier of LLDP frames. The device information on the neighboring devices ages out and is discarded when its corresponding TTL expires. The TTL value is to multiply the TTL multiplier by the LLDP frames transmitting interval.
Port Description TLV	This displays the remote port description.
System Name TLV	This displays the system name of the remote device.
System Description TLV	This displays the system description of the remote device.
System Capabilities TLV	This displays whether the system capabilities are enabled and supported on the remote device. • System Capabilities Supported • System Capabilities Enabled
Management Address TLV	This displays the following management address parameters of the remote device. • Management Address Subtype • Management Address • Interface Number Subtype • Interface Number • Object Identifier

Figure 195 Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail> (Dot 1 and Dot3 TLV)



Dot1 TLV		
Port VLAN ID TLV	Port VLAN ID	100
Port-Protocol VLAN ID TLV	Port-Protocol VLAN ID	200
	Port-Protocol VLAN ID Supported	Yes
	Port-Protocol VLAN ID Enabled	Yes
Vlan Name TLV	VLAN ID	1
	VLAN Name	client 1
Protocol Identity TLV	Protocol ID	1
Dot3 TLV		
MAC PHY Configuration & Status TLV	AN Supported	Yes
	AN Enabled	Yes
	AN Advertised Capability	10baseT 10baseTFD 100baseTX 100baseTXFD 1000baseTFD
	Oper MAU type	30
Link Aggregation TLV	Aggregation Capability	Yes
	Aggregation Status	Yes
	Aggregated Port ID	1
Power Via MDI TLV	Port Class	PSE
	MDI Supported	Yes
	MDI Enabled	Yes
	Pair Controlable	No
	PSE Power Pairs	1
	Power Class	1
Max Frame Size TLV	Max Frame Size	1518

The following table describes the labels in the Dot1 and Dot3 parts of the screen.

Table 136 Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail (Dot1 and Dot3 TLV)

LABEL	DESCRIPTION
Dot1 TLV	
Port VLAN ID TLV	This displays the VLAN ID of this port on the remote device.
Port-Protocol VLAN ID TLV	This displays the IEEE 802.1 Port Protocol VLAN ID TLV, which indicates whether the VLAN ID and whether it is enabled and supported on the port of remote Switch which sent the LLDPDU. • Port-Protocol VLAN ID • Port-Protocol VLAN ID Supported • Port-Protocol VLAN ID Enabled
Vlan Name TLV	This shows the VLAN ID and name for remote device port. • VLAN ID • VLAN Name

Table 136 Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail (Dot1 and Dot3 TLV)

LABEL	DESCRIPTION
Protocol Identity TLV	The Protocol Identity TLV allows the Switch to advertise the particular protocols that are accessible through its port.
Dot3 TLV	
MAC PHY Configuration & Status TLV	The MAC/PHY Configuration/Status TLV advertises the bit-rate and duplex capability of the sending 802.3 node. It also advertises the current duplex and bit-rating of the sending node. Lastly, it advertises whether these setting were the result of auto-negotiation during link initiation or manual override. • AN Supported - Displays if the port supports or does not support auto-negotiation. • AN Enabled - The current auto-negotiation status of the port. • AN Advertised Capability - The auto-negotiation capabilities of the port. • Oper MAU Type - The current Medium Attachment Unit (MAU) type of the port
Link Aggregation TLV	The Link Aggregation TLV indicates whether the link is capable of being aggregated, whether the link is currently in an aggregation, and if in an aggregation, the port identification of the aggregation. • Aggregation Capability — The current aggregation capability of the port. • Aggregation Status — The current aggregation status of the port. • Aggregation Port ID — The aggregation ID of the current port.
Power Via MDI TLV	The Power Via MDI TLV allows network management to advertise and discover the MDI power support capabilities of the sending port on the remote device. • Port Class • MDI Supported • MDI Enabled • Pair Controlable • PSE Power Pairs • Power Class
Max Frame Size TLV	This displays the maximum supported frame size in octets.

Figure 196 Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail (MED TLV)

MED TLV

Capabilities TLV	Network Policy	Yes
	Location	Yes
	Extend Power via MDI PSE	No
	Extend Power via MDI PD	No
	Inventory Management	No
Device Type TLV	Device Type	Network Connectivity
Network Policy TLV	Voice	VLAN ID 10, tagged, known, L2-priority 7, DSCP 63
	Voice-Signaling	VLAN ID 100, tagged, known, L2-priority 2, DSCP 10
	Guest-Voice	VLAN ID 20, tagged, known, L2-priority 3, DSCP 12
	Guest-Voice-Signaling	VLAN ID 0, untagged, known, L2-priority 0, DSCP 0
	Softphone-Voice	VLAN ID 200, tagged, known, L2-priority 1, DSCP 1
	Video-Conferencing	VLAN ID 0, untagged, known, L2-priority 0, DSCP 0
	Streaming-Video	VLAN ID 300, tagged, known, L2-priority 4, DSCP 20
	Video-Signaling	VLAN ID 400, tagged, known, L2-priority 6, DSCP 55
Location Identification TLV	Coordinate-base LCI	latitude north 0.0 longitude east 0.9995 altitude meters 0.0 datum NAD83-MLLW
	Civic LCI	country TW city HSINCHU building ZYXEL
	ELIN	1234567890
Inventory TLV	Hardware Revision	V20131114 | 11/14/2013
	Software Revision	V4.10(AAOA.0) | 11/15/2013
	Firmware Revision	V4.10(AAOA.0) | 11/15/2013
	Model Name	GS3700-HP
	Manufacturer	123456789

The following table describes the labels in the MED TLV part of the screen.

Table 137 Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail (MED TLV)

LABEL	DESCRIPTION
MED TLV	LLDP Media Endpoint Discovery (MED) is an extension of LLDP that provides additional capabilities to support media endpoint devices. MED enables advertisement and discovery of network policies, device location discovery to allow creation of location databases, and information for troubleshooting.
Capabilities TLV	This displays the MED capabilities the remote port supports. • Network Policy • Location • Extend Power via MDI PSE • Extend Power via MDI PD • Inventory Management
Device Type TLV	LLDP-MED endpoint device classes: • Endpoint Class I • Endpoint Class II • Endpoint Class III • Network Connectivity
Network Policy TLV	This displays a network policy for the specified application. • Voice • Voice-Signaling • Guest-Voice • Guest-Voice-Signaling • Softphone-Voice • Video-Conferencing • Streaming-Video • Video-Signaling
Location Identification TLV	This shows the location information of a caller by its: • Coordinate-base LCI - latitude and longitude coordinates of the Location Configuration Information (LCI) • Civic LCI - IETF Geopriv Civic Address based Location Configuration Information • ELIN - (Emergency Location Identifier Number)

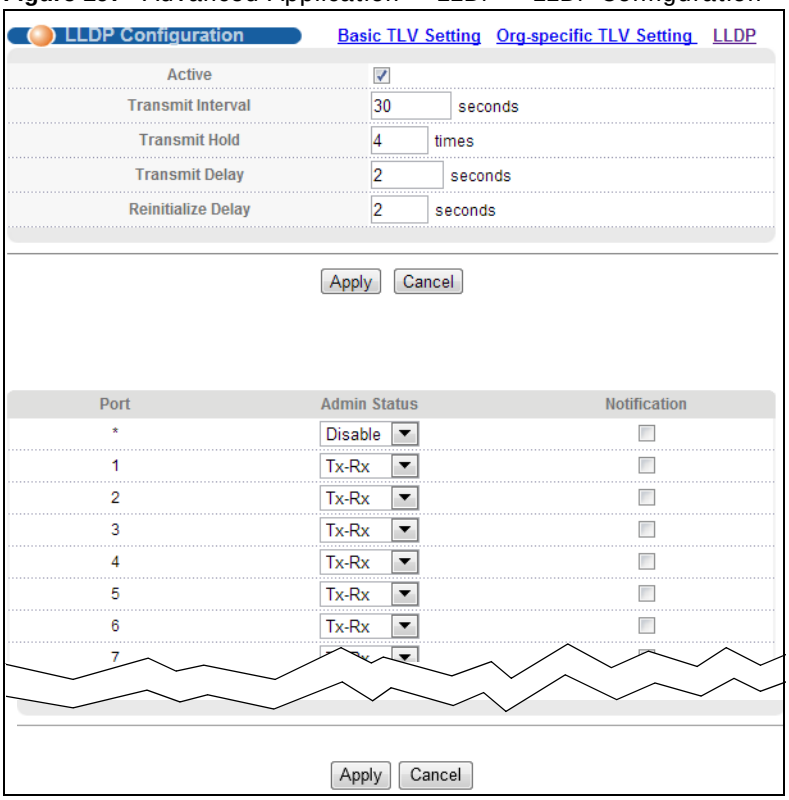
Table 137 Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail (MED TLV)

LABEL	DESCRIPTION
Inventory TLV	The majority of IP Phones lack support of management protocols such as SNMP, so LLDP-MED inventory TLVs are used to provide their inventory information to the Network Connectivity Devices such as the Switch. The Inventory TLV may contain the following information. • Hardware Revision • Software Revision • Firmware Revision • Model Name • Manufacturer • Serial Number • Asset ID
Extended Power via MDI TLV	Extended Power Via MDI Discovery enables detailed power information to be advertised by Media Endpoints, such as IP phones and Network Connectivity Devices such as the Switch. • Power Type - whether it is currently operating from primary power or is on backup power (backup power may indicate to the Endpoint Device that it should move to a power conservation mode). • Power Source - whether or not the Endpoint is currently operating from an external power source. • Power Priority - the Endpoint Device's power priority (which the Network Connectivity Device may use to prioritize which devices will remain in service during power shortages) • Power Value - power requirement, in fractions of Watts, in current configuration

34.6 LLDP Configuration

Use this screen to configure global LLDP settings on the Switch. Click **Advanced Application** > **LLDP > LLDP Configuration (Click Here)** to display the screen as shown next.

Figure 197 Advanced Application > LLDP > LLDP Configuration



The following table describes the labels in this screen.

Table 138 Advanced Application > LLDP > LLDP Configuration

LABEL	DESCRIPTION
Active	Select to enable LLDP on the Switch. It is enabled by default.
Transmit Interval	Enter how many seconds the Switch waits before sending LLDP packets.
Transmit Hold	Enter the time-to-live (TTL) multiplier of LLDP frames. The device information on the neighboring devices ages out and is discarded when its corresponding TTL expires. The TTL value is to multiply the TTL multiplier by the LLDP packets transmitting interval.
Transmit Delay	Enter the delay (in seconds) between successive LLDPDU transmissions initiated by value or status changes in the Switch MIB.
Reinitialize Delay	Enter the number of seconds for LLDP to wait before initializing on a port.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Port	This displays the port number with this LLDP configuration. * means all ports.
Admin Status	Select whether LLDP transmission and/or reception is allowed on this port. • Disable - not allowed • Tx-Only - transmit only • Rx-Only - receive only • Tx-Rx - transmit and receive
Notification	Select whether LLDP notification is enabled on this port.

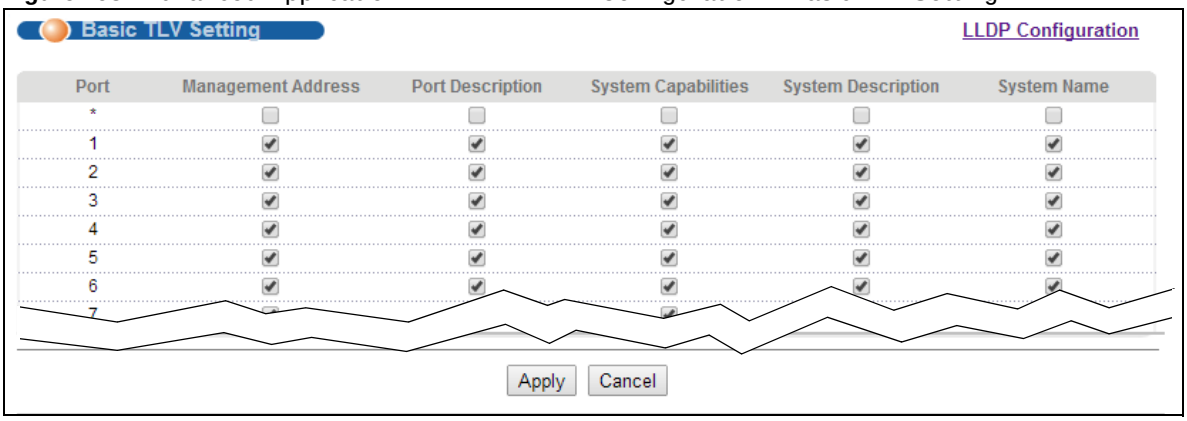
Table 138 Advanced Application > LLDP > LLDP Configuration

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

34.6.1 LLDP Configuration Basic TLV Setting

Use this screen to configure Basic TLV settings. Click **Advanced Application** > **LLDP > LLDP Configuration (Click Here) > Basic TLV Setting** to display the screen as shown next.

Figure 198 Advanced Application > LLDP > LLDP Configuration> Basic TLV Setting



The following table describes the labels in this screen.

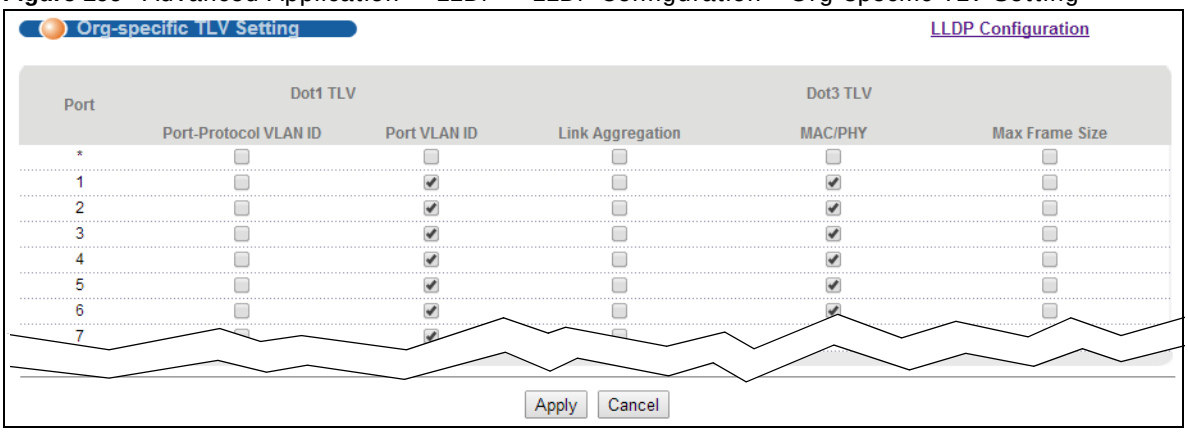
Table 139 Advanced Application > LLDP > LLDP Configuration > Basic TLV Setting

LABEL	DESCRIPTION
Port	This displays the port number on which you're configuring LLDP . Select check boxes in the * row to configure all ports simultaenously. All check boxes below * row are enabled by default.
Management Address	Select check box to enable or disable the sending of Management Address TLVs on the port(s).
Port Description	Select check box to enable or disable the sending of Port Description TLVs on the port(s).
System Capabilities	Select check box to enable or disable the sending of System Capabilities TLVs on the port(s).
System Description	Select check box to enable or disable the sending of System Description TLVs on the port(s).
System Name	Select check box to enable or disable the sending of System Name TLVs on the port(s).
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

34.6.2 LLDP Configuraion Basic Org-specific TLV Setting

Use this screen to configure organization-specific TLV settings. Click **Advanced Application** > **LLDP > LLDP Configuration (Click Here) > Org-specific TLV Setting** to display the screen as shown next.

Figure 199 Advanced Application > LLDP > LLDP Configuration> Org-specific TLV Setting



The following table describes the labels in this screen.

Table 140 Advanced Application > LLDP > LLDP Configuration > Org-specific TLV Setting

LABEL	DESCRIPTION
Port	This displays the port number on which you're configuring LLDP . Select check boxes in the * row to configure all ports simultaenously.
Dot1 TLV	
Port-Protocol VLAN ID	Select check box to enable or disable the sending of IEEE 802.1 Port and Protocol VLAN ID TLVs on the port(s).
Port VLAN ID	Select check box to enable or disable the sending of IEEE 802.1 Port VLAN ID TLVs on the port(s). All check boxes in this column are enabled by default.
Dot3 TLV	
Power Via MDI TLV	**Note**: For PoE models only. The Power Via MDI TLV allows network management to advertise and discover the MDI power support capabilities of the sending port on the remote device. • Port Class • MDI Supported • MDI Enabled • Pair Controlable • PSE Power Pairs • Power Class
Link Aggregation	Select check box to enable or disable the sending of IEEE 802.3 Link Aggregation TLVs on the port(s).
MAC/PHY	Select check box to enable or disable the sending of IEEE 802.3 MAC/PHY Configuration/ Status TLVs on the port(s). All check boxes in this column are enabled by default.
Max Frame Size	Select check box to enable or disable the sending of IEEE 802.3 Max Frame Size TLVs on the port(s).

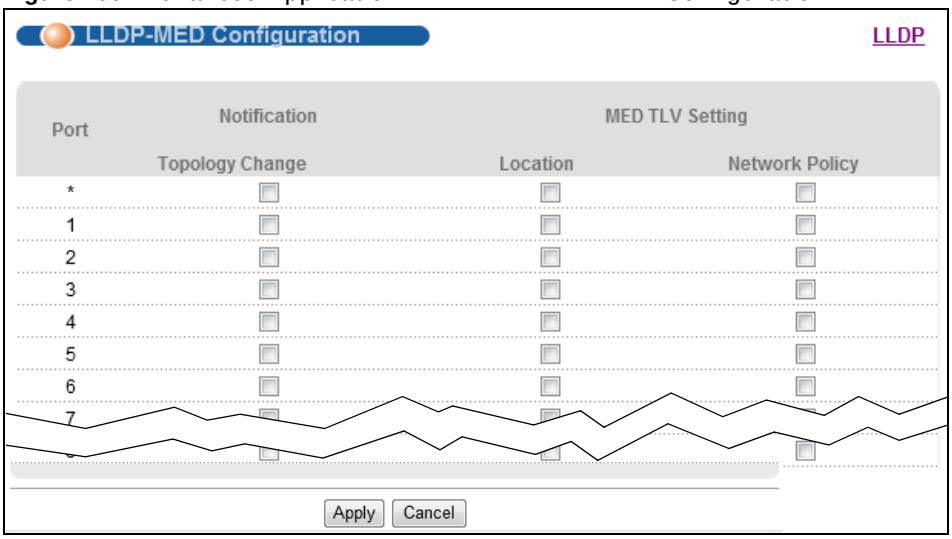
Table 140 Advanced Application > LLDP > LLDP Configuration > Org-specific TLV Setting

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

34.7 LLDP-MED Configuration

Click **Advanced Application** > **LLDP > LLDP-MED Configuration (Click Here)** to display the screen as shown next.

Figure 200 Advanced Application > LLDP > LLDP-MED Configuration



The following table describes the labels in this screen.

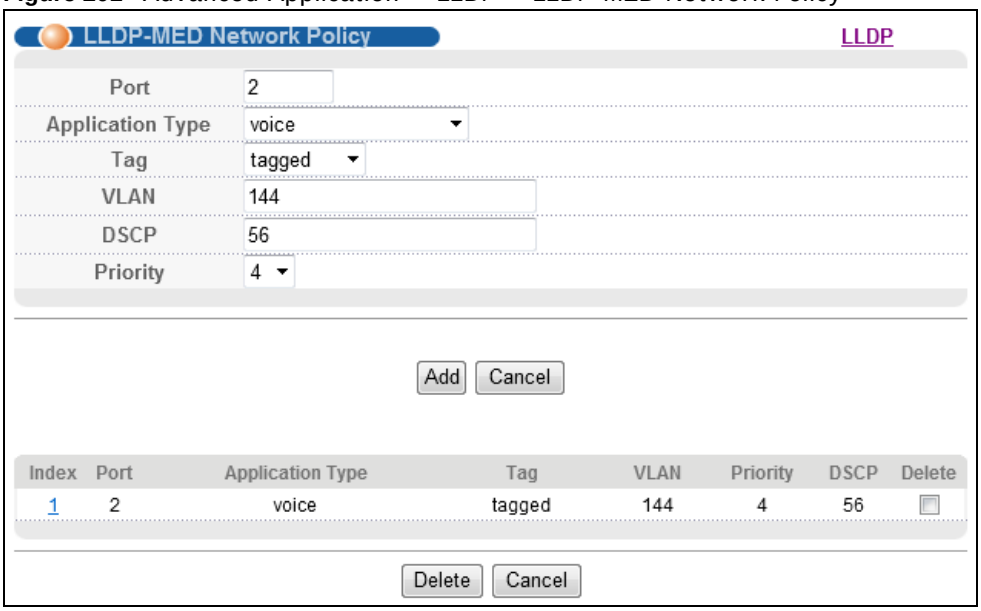
Table 141 Advanced Application > LLDP > LLDP-MED Configuration

LABEL	DESCRIPTION
Port	This displays the port number on which you're configuring LLDP-MED. Select * to configure all ports simultaneously.
Notification	
Topology Change	Select to enable LLDP-MED topology change traps on this port.
MED TLV Setting	
Location	Select to enable transmitting LLDP-MED location TLV.
Network Policy	Select to enable transmitting LLDP-MED Network Policy TLV.
Apply	Click Apply to save the changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

34.8 LLDP-MED Network Policy

Click **Advanced Application** > **LLDP > LLDP-MED Network Policy (Click Here)** to display the screen as shown next.

Figure 201 Advanced Application > LLDP > LLDP-MED Network Policy



The following table describes the labels in this screen.

Table 142 Advanced Application > LLDP > LLDP-MED Network Policy

LABEL	DESCRIPTION
Port	Enter the port number to set up the LLDP-MED network policy.
Application Type	Select the type of application used in the network policy. • voice • voice-signaling • guest-voice • guest-voice-signaling • softphone-voice • video-conferencing • streaming-video • video-signaling
Tag	Select to tag or untag in the network policy. • tagged • untagged
VLAN	Enter the VLAN ID number. It should be from 1 to 4094. For priority tagged frames, enter “0”.
DSCP	Enter the DSCP value of the network policy. The value is defined from 0 through 63 with the 0 representing use of the default DSCP value.
Priority	Enter the priority value for the network policy.
Add	Click Add after finish entering the network policy information. A summary table will list all the Switch you’ve added.
Cancel	Click Cancel to begin entering the information afresh.

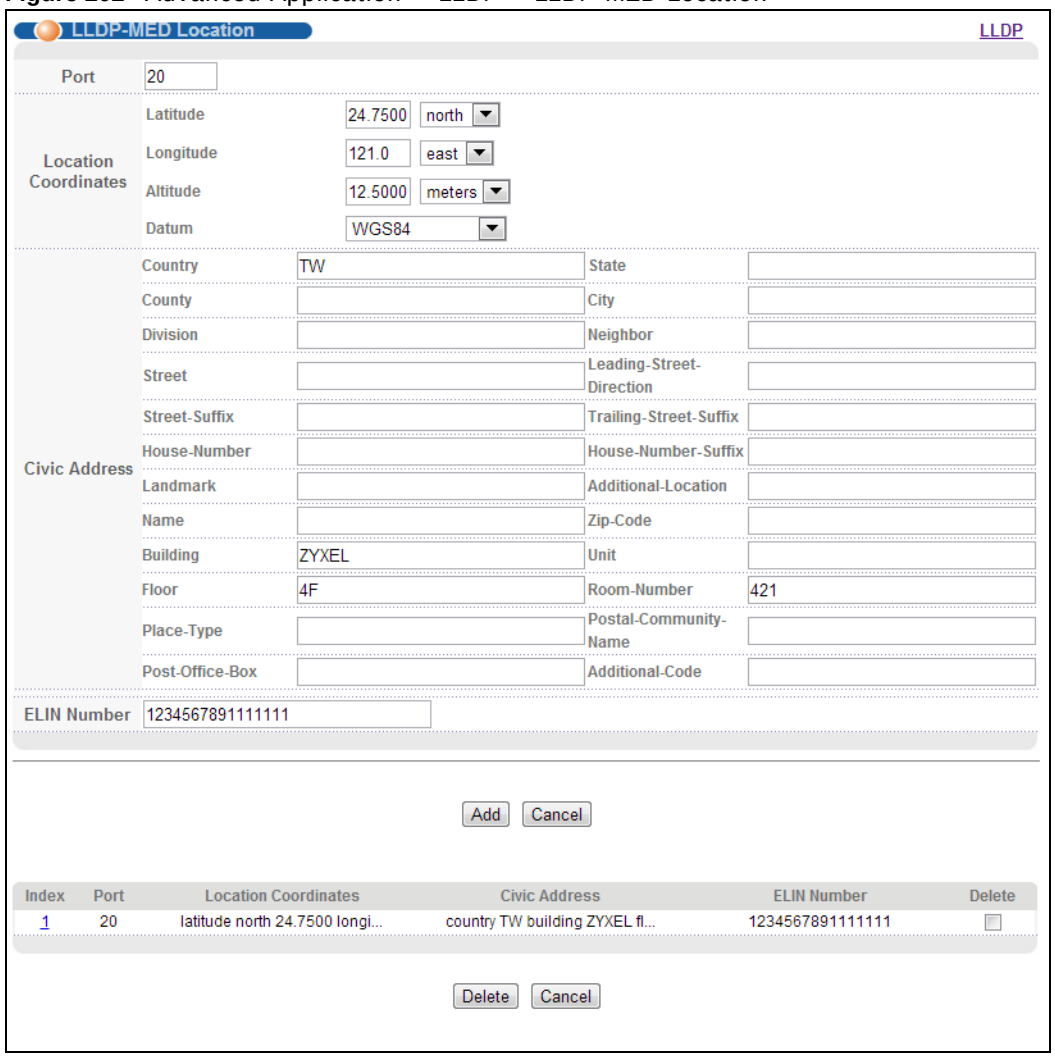
Table 142 Advanced Application > LLDP > LLDP-MED Network Policy

LABEL	DESCRIPTION
Index	This field displays the of index number of the network policy. Click an index number to edit the rule.
Port	This field displays the port number of the network policy.
Application Type	This field displays the application type of the network policy.
Tag	This field displays the Tag Status of the network policy.
VLAN	This field displays the VLANID of the network policy.
Priority	This field displays the priority value of the network policy.
DSCP	This field displays the DSCP value of the network policy.
Delete	Check the rules that you want to remove in the delete column, then click the Delete button.
Cancel	Click Cancel to clear the selected checkboxes in the **Delete** column.

34.9 LLDP-MED Location

Click **Advanced Application** > **LLDP > LLDP-MED Location (Click Here)** to display the screen as shown next.

Figure 202 Advanced Application > LLDP > LLDP-MED Location



The following table describes the labels in this screen.

Table 143 Advanced Application > LLDP > LLDP-MED Location

LABEL	DESCRIPTION
Port	Enter the port number you want to set up the location within the LLDP-MED network.
Location Coordinates	The LLDP-MED uses geographical coordinates and Civic Address to set the location information of the remote device. Geographical based coordinates includes latitude, longitude, altitude and datum. Civic Address includes Country, State, County, City, Street and other related information.
Latitude	Enter the latitude information. The value should be from 0º to 90º. The negative value represents the South. • north • south
Longitude	Enter the longitude information. The value should be from 0º to 180º. The negative value represents the West. • west • east

Table 143 Advanced Application > LLDP > LLDP-MED Location

LABEL	DESCRIPTION
Altitude	Enter the altitude information. The value should be from -2097151 to 2097151 in meters or in floors. • meters • floor
Datum	Select the appropriate geodetic datum used by GPS. • WGS84 • NAD83-NAVD88 • NAD83-MLLW
Civic Address	Enter the Civic Address by providing information such as Country, State, County, City, Street, Number, ZIP code and other additional information. Enter at least two field in this configuration including the Country. The valid length of the Country field is 2 characters and all other fields are up to 32 characters. • Country • State • County • City • Division • Neighbor • Street • Leading-Street-Direction • Street-Suffix • Trailing-Street-Suffix • House-Number • House-Number-Suffix • Landmark • Additional-Location • Name • Zip-Code • Building • Unit • Floor • Room-Number • Place-Type • Postal-Community-Name • Post-Office-Box • Additional-Code
ELIN Number	Enter a numerical digit string, corresponding to the ELIN identifier which is used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. The valid length is from 10 to 25 characters.
Add	Click Add after finish entering the location information.
Cancel	Click Cancel to begin entering the location information afresh.
Index	This lists the index number of the location configuration. Click an index number to view or edit the location.
Port	This lists the port number of the location configuration.
Location Coordinates	This field displays the location configuration information based on geographical coordinates that includes longitude, latitude, altitude and datum.
Civic Address	This field displays the Civic Address for the remote device using information such as Country, State, County, City, Street, Number, ZIP code and additional information.
ELIN Number	This field shows the Emergency Location Identification Number (ELIN), which is used to identify endpoint devices when they issue emergency call services. The valid length is from 10 to 25 characters.

Table 143 Advanced Application > LLDP > LLDP-MED Location

LABEL	DESCRIPTION
Delete	Check the locations that you want to remove in the Delete column, then click the Delete button.
Cancel	Click Cancel to clear the selected check boxes in the delete column.

35

Static Route

35.1 Static Route Overview

This chapter shows you how to configure static routes.

The Switch uses IP for communication with management computers, for example using HTTP, or SNMP. Use IP static routes to have the Switch respond to remote management stations that are not reachable through the default gateway. The Switch can also use static routes to send data to a server or device that is not reachable through the default gateway, for example when sending SNMP traps or using ping to test IP connectivity.

35.1.1 What You Can Do

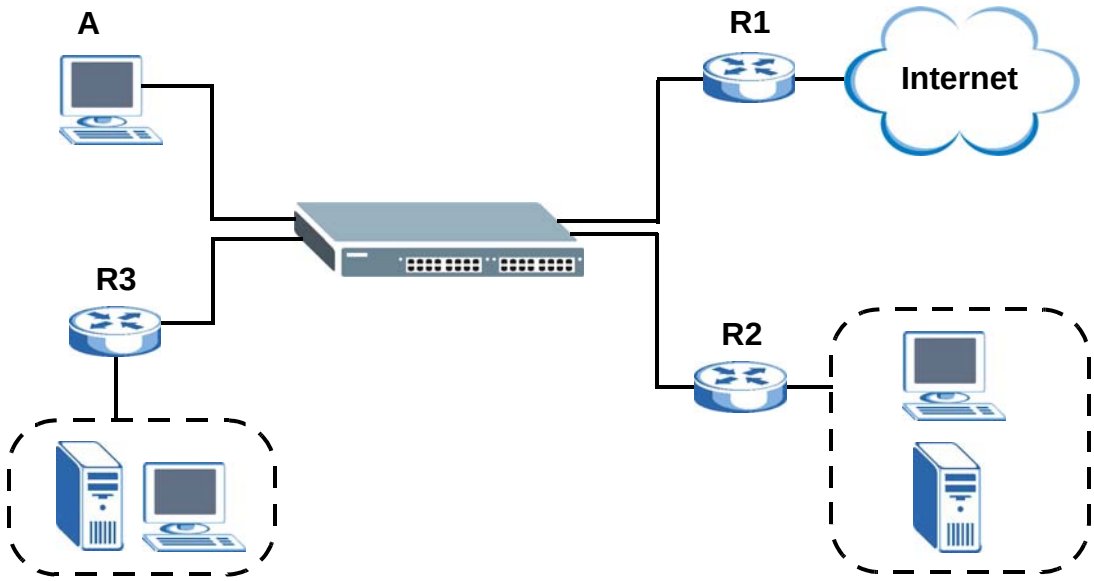
- Use **IPv4 Static Route** to open a screen where you can create IPv4 static routing rules.
- Use **IPv6 Static Route** to open a screen where you can create IPv6 static routing rules.

35.2 Static Routing

The Switch usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the Switch send data to devices not reachable through the default gateway, use static routes.

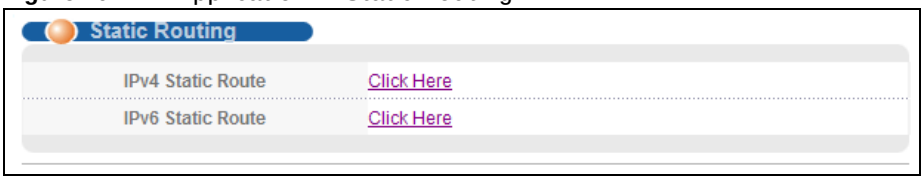
For example, the next figure shows a computer (**A**) connected to the Switch. The Switch routes most traffic from **A** to the Internet through the Switch's default gateway (**R1**). You create one static route to connect to services offered by your ISP behind router **R2**. You create another static route to communicate with a separate network behind a router **R3** connected to the Switch.

Figure 203 Example of Static Routing Topology



Click **IP Application** > **Static Routing** in the navigation panel to display the screen as shown. Click the link next to **IPv4 Static Route** to open a screen where you can create IPv4 static routing rules. Click the link next to **IPv6 Static Route** to open a screen where you can create IPv6 static routing rules.

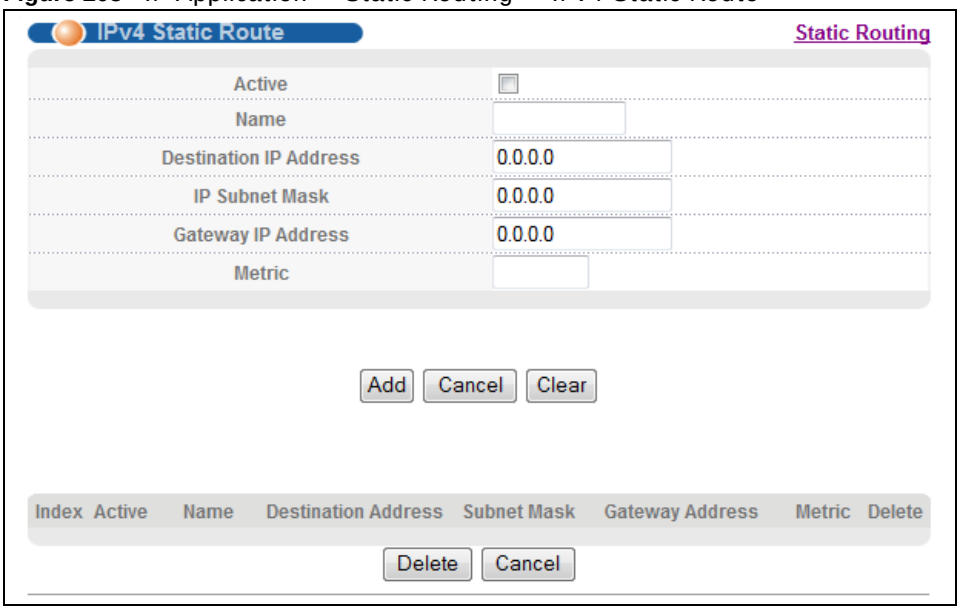
Figure 204 IP Application > Static Routing



35.3 Configuring Static Routing

Click **IP Application > Static Routing > IPv4 Static Route** in the navigation panel to display the screen as shown.

Figure 205 IP Application > Static Routing > IPv4 Static Route



The following table describes the related labels you use to create a static route.

Table 144 IP Application > Static Routing > IPv4 Static Route

LABEL	DESCRIPTION
Active	This field allows you to activate/deactivate this static route.
Name	Enter a descriptive name (up to 10 printable ASCII characters) for identification purposes.
Destination IP Address	This parameter specifies the IP network address of the final destination.
IP Subnet Mask	Enter the subnet mask for this destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your Switch that will forward the packet to the destination. The gateway must be a router on the same segment as your Switch.
Metric	The metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Add	Click **Add** to insert a new static route to the Switch’s run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the above fields to your previous configuration.
Clear	Click **Clear** to set the above fields back to the factory defaults.
Index	This field displays the index number of the route. Click a number to edit the static route entry.
Active	This field displays **Yes** when the static route is activated and **NO** when it is deactivated.
Name	This field displays the descriptive name for this route. This is for identification purposes only.
Destination Address	This field displays the IP network address of the final destination.
Subnet Mask	This field displays the subnet mask for this destination.

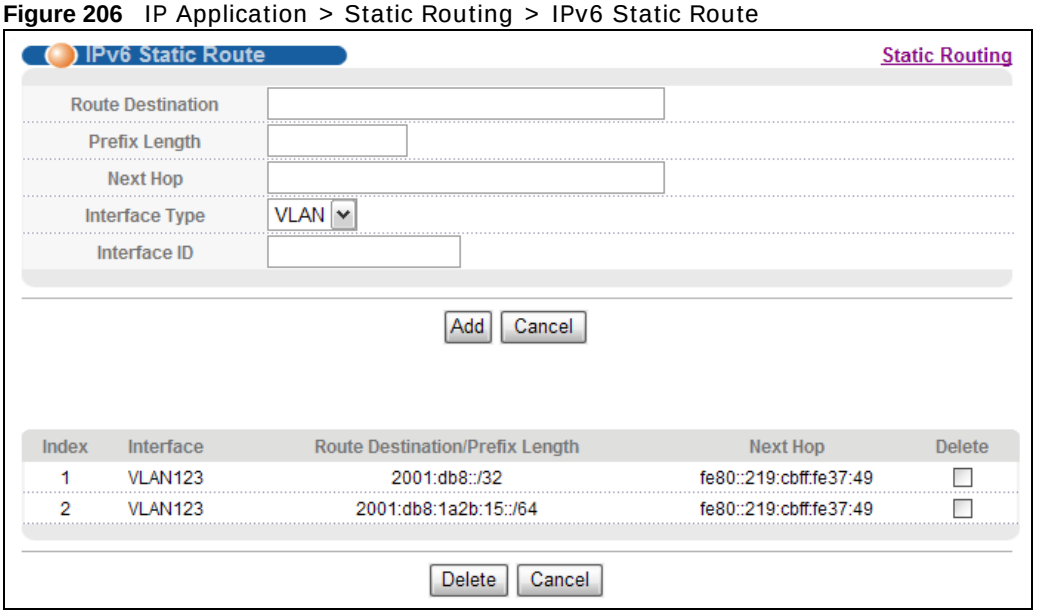
Table 144 IP Application > Static Routing > IPv4 Static Route (continued)

LABEL	DESCRIPTION
Gateway Address	This field displays the IP address of the gateway. The gateway is an immediate neighbor of your Switch that will forward the packet to the destination.
Metric	This field displays the cost of transmission for routing purposes.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

35.4 Configuring IPv6 Static Routing

Click the link next to **IPv6 Static Route** in the **IP Application** > **Static Routing** screen to display the screen as shown.

Figure 206 IP Application > Static Routing > IPv6 Static Route



The following table describes the related labels you use to create a static route.

Table 145 IP Application > Static Routing > IPv6 Static Route

LABEL	DESCRIPTION
Route Destination	Enter the IPv6 address of the final destination.
Prefix Length	Enter the prefix length number of up to 64 for this destination.
Next Hop	Enter the IPv6 address of the next-hop router.
Interface Type	Select the type of the IPv6 interface through which the IPv6 packets are forwarded. The Switch supports only the VLAN interface type at the time of writing.
Interface ID	Enter the ID number of the IPv6 interface through which the IPv6 packets are forwarded.
Add	Click **Add** to insert a new static route to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

Table 145 IP Application > Static Routing > IPv6 Static Route (continued)

LABEL	DESCRIPTION
Index	This field displays the index number of the route. Click a number to edit the static route entry.
Interface	This field displays the descriptive name of the interface that is used to forward the packets to the destination.
Route Destination/ Prefix Length	This field displays the IPv6 subnet prefix and prefix length of the final destination.
Next Hop	This field displays the IPv6 address of the gateway that helps forward the packet to the destination.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

36

Differentiated Services

36.1 Differentiated Services Overview

This chapter shows you how to configure Differentiated Services (DiffServ) on the Switch.

Quality of Service (QoS) is used to prioritize source-to-destination traffic flows. All packets in the flow are given the same priority. You can use CoS (class of service) to give different priorities to different packet types.

DiffServ is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

36.1.1 What You Can Do

- Use the **DiffServ** screen (Section 36.2 on page 297) to activate DiffServ to apply marking rules or IEEE 802.1p priority mapping on the Switch.
- Use the **DSCP** screen (Section 36.3.1 on page 299) to change the DSCP-IEEE 802.1p mapping.

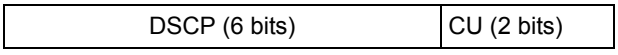
36.1.2 What You Need to Know

Read on for concepts on Differentiated Services that can help you configure the screens in this chapter.

DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (ToS) field in the IP header. The DS field contains a 6-bit DSCP field which can define up to 64 service levels and the remaining 2 bits are defined as currently unused (CU). The following figure illustrates the DS field.

Figure 207 DiffServ: Differentiated Service Field



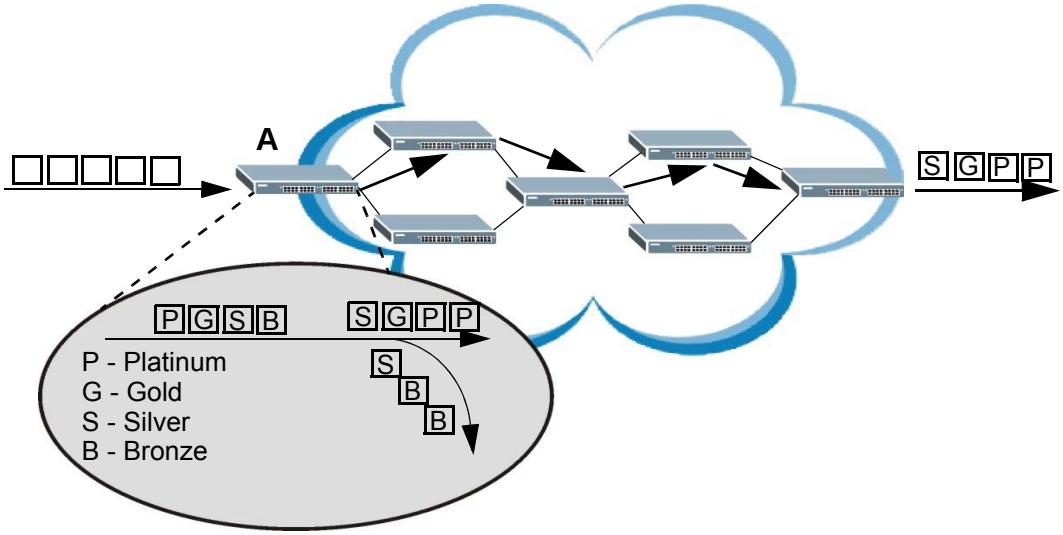
DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

The DSCP value determines the PHB (Per-Hop Behavior), that each packet gets as it is forwarded across the DiffServ network. Based on the marking rule different kinds of traffic can be marked for different priorities of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

DiffServ Network Example

The following figure depicts a DiffServ network consisting of a group of directly connected DiffServ-compliant network devices. The boundary node (**A** in Figure 208) in a DiffServ network classifies (marks with a DSCP value) the incoming packets into different traffic flows (**Platinum**, **Gold**, **Silver**, **Bronze**) based on the configured marking rules. A network administrator can then apply various traffic policies to the traffic flows. An example traffic policy, is to give higher drop precedence to one traffic flow over others. In our example, packets in the **Bronze** traffic flow are more likely to be dropped when congestion occurs than the packets in the **Platinum** traffic flow as they move across the DiffServ network.

Figure 208 DiffServ Network

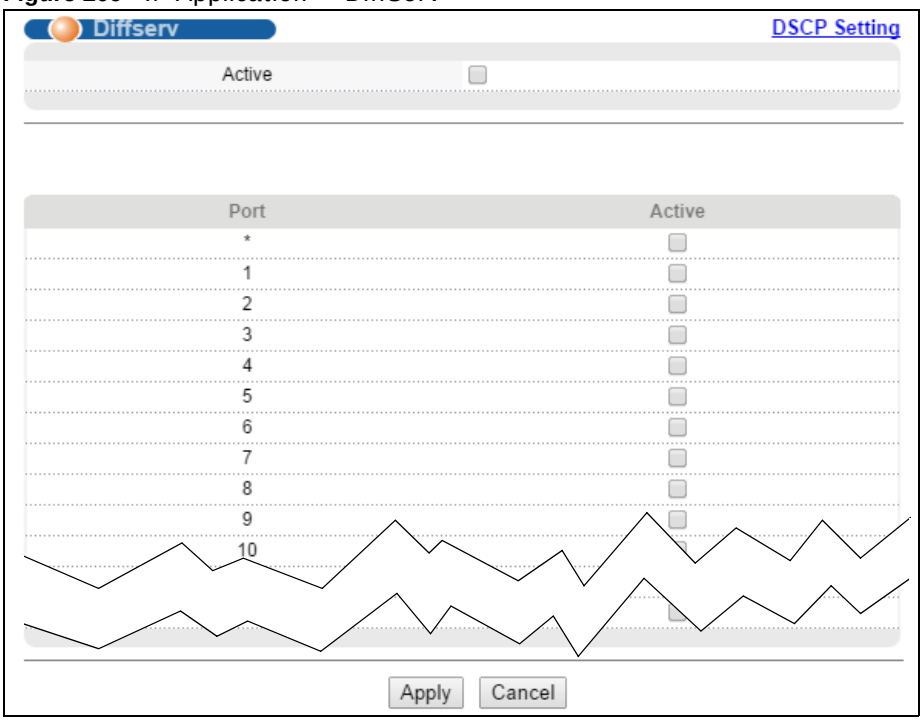


36.2 Activating DiffServ

Activate DiffServ to apply marking rules or IEEE 802.1p priority mapping on the Switch.

Click **IP Application** > **DiffServ** in the navigation panel to display the screen as shown.

Figure 209 IP Application > DiffServ



The following table describes the labels in this screen.

Table 146 IP Application > DiffServ

LABEL	DESCRIPTION
Active	Select this option to enable DiffServ on the Switch.
Port	This field displays the index number of a port on the switch.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Changes in this row are copied to all the ports as soon as you make them.
Active	Select **Active** to enable Diffserv on the port.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

36.3 DSCP-to-IEEE 802.1p Priority Settings

You can configure the DSCP to IEEE 802.1p mapping to allow the Switch to prioritize all traffic based on the incoming DSCP value according to the DiffServ to IEEE 802.1p mapping table.

The following table shows the default DSCP-to-IEEE802.1p mapping.

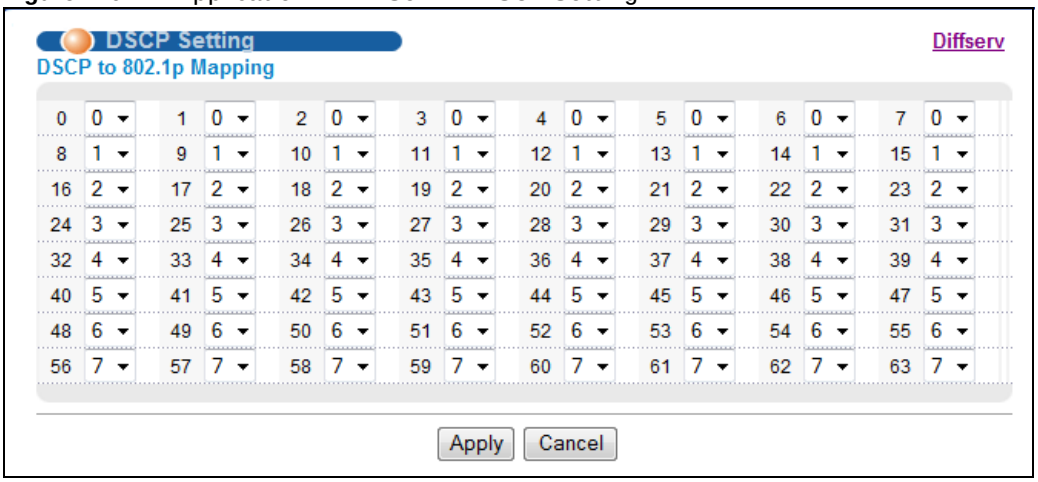
Table 147 Default DSCP-IEEE 802.1p Mapping

DSCP VALUE	0 – 7	8 – 15	16 – 23	24 – 31	32 – 39	40 – 47	48 – 55	56 – 63
IEEE 802.1p	0	1	2	3	4	5	6	7

36.3.1 Configuring DSCP Settings

To change the DSCP-IEEE 802.1p mapping click the **DSCP Setting** link in the **DiffServ** screen to display the screen as shown next.

Figure 210 IP Application > DiffServ > DSCP Setting



The following table describes the labels in this screen.

Table 148 IP Application > DiffServ > DSCP Setting

LABEL	DESCRIPTION
0 ... 63	This is the DSCP classification identification number. To set the IEEE 802.1p priority mapping, select the priority level from the drop-down list box.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

37

DHCP

37.1 DHCP Overview

This chapter shows you how to configure the DHCP feature.

DHCP (Dynamic Host Configuration Protocol RFC 2131 and RFC 2132) allows individual computers to obtain TCP/IP configuration at start-up from a server. If you configure the Switch as a DHCP relay agent, then the Switch forwards DHCP requests to DHCP server on your network. If you don't configure the Switch as a DHCP relay agent then you must have a DHCP server in the broadcast domain of the client computers or else the client computers must be configured manually.

37.1.1 What You Can Do

- Use the **DHCPv4 Status** screen (Section 37.3 on page 302) to display the relay mode.
- Use the **DHCPv4 Relay** screen (Section 37.4 on page 302) to enable and configure global DHCP relay.
- Use the **VLAN Setting** screen (Section 37.5 on page 308) to configure your DHCP settings based on the VLAN domain of the DHCP clients.
- Use the **DHCPv6 Relay** screen (Section 37.6 on page 311) to enable and configure DHCPv6 relay.

37.1.2 What You Need to Know

Read on for concepts on DHCP that can help you configure the screens in this chapter.

DHCP Modes

If there is already a DHCP server on your network, then you can configure the Switch as a DHCP relay agent. When the Switch receives a request from a computer on your network, it contacts the DHCP server for the necessary IP information, and then relays the assigned information back to the computer.

DHCP Configuration Options

The DHCP configuration on the Switch is divided into **Global** and **VLAN** screens. The screen you should use for configuration depends on the DHCP services you want to offer the DHCP clients on your network. Choose the configuration screen based on the following criteria:

- **Global** - The Switch forwards all DHCP requests to the same DHCP server.
- **VLAN** - The Switch is configured on a VLAN by VLAN basis. The Switch can be configured to relay DHCP requests to different DHCP servers for clients in different VLAN.

DHCP Relay

Configure DHCP relay on the Switch if the DHCP clients and the DHCP server are not in the same broadcast domain. During the initial IP address leasing, the Switch helps to relay network information (such as the IP address and subnet mask) between a DHCP client and a DHCP server. Once the DHCP client obtains an IP address and can connect to the network, network information renewal is done between the DHCP client and the DHCP server without the help of the Switch.

The Switch can be configured as a global DHCP relay. This means that the Switch forwards all DHCP requests from all domains to the same DHCP server. You can also configure the Switch to relay DHCP information based on the VLAN membership of the DHCP clients.

DHCP Relay Agent Information

The Switch can add information about the source of client DHCP requests that it relays to a DHCP server by adding **Relay Agent Information**. This helps provide authentication about the source of the requests. The DHCP server can then provide an IP address based on this information. Please refer to RFC 3046 for more details.

The DHCP **Relay Agent Information** feature adds an Agent Information field to the **Option 82** field. The **Option 82** field is in the DHCP headers of client DHCP request frames that the Switch relays to a DHCP server.

Relay Agent Information can include the **System Name** of the Switch if you select this option. You can change the **System Name** in **Basic Settings** > **General Setup**.

The following describes the DHCP relay information that the Switch sends to the DHCP server:

Table 149 Relay Agent Information

FIELD LABELS	DESCRIPTION
Slot ID	(1 byte) This value is always 0 for stand-alone switches.
Port ID	(1 byte) This is the port that the DHCP client is connected to.
VLAN ID	(2 bytes) This is the VLAN that the port belongs to.
Information	(up to 64 bytes) This optional, read-only field is set according to system name set in **Basic Settings > General Setup.**

37.2 DHCP Configuration

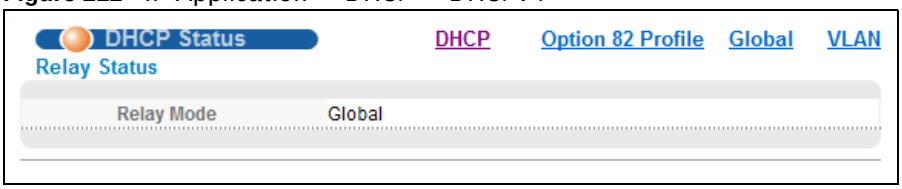
Click **IP Application** > **DHCP** in the navigation panel to display the screen as shown. Click the link next to **DHCPv4** to open screens where you can enable and configure DHCPv4 relay settings and create option 82 profiles. Click the link next to **DHCPv6** to open a screen where you can configure DHCPv6 relay settings.

Figure 211 IP Application > DHCP

37.3 DHCPv4 Status

Click **IP Application** > **DHCP > DHCPv4** in the navigation panel. The **DHCP Status** screen displays.

Figure 212 IP Application > DHCP > DHCPv4



The following table describes the labels in this screen.

Table 150 IP Application > DHCP > DHCPv4

LABEL	DESCRIPTION
Relay Status	This section displays configuration settings related to the Switch's DHCP relay mode.
Relay Mode	This field displays: **None** - if the Switch is not configured as a DHCP relay agent. **Global** - if the Switch is configured as a DHCP relay agent only. **VLAN** - followed by a VLAN ID or multiple VLAN IDs if it is configured as a relay agent for specific VLAN(s).

37.4 DHCPv4 Relay

Configure DHCP relay on the Switch if the DHCP clients and the DHCP server are not in the same broadcast domain. During the initial IP address leasing, the Switch helps to relay network information (such as the IP address and subnet mask) between a DHCP client and a DHCP server. Once the DHCP client obtains an IP address and can connect to the network, network information renewal is done between the DHCP client and the DHCP server without the help of the Switch.

The Switch can be configured as a global DHCP relay. This means that the Switch forwards all DHCP requests from all domains to the same DHCP server. You can also configure the Switch to relay DHCP information based on the VLAN membership of the DHCP clients.

37.4.1 DHCPv4 Relay Agent Information

The Switch can add information about the source of client DHCP requests that it relays to a DHCP server by adding **Relay Agent Information**. This helps provide authentication about the source of the requests. The DHCP server can then provide an IP address based on this information. Please refer to RFC 3046 for more details.

The DHCP **Relay Agent Information** feature adds an Agent Information field (also known as the **Option 82** field) to DHCP requests. The **Option 82** field is in the DHCP headers of client DHCP request frames that the Switch relays to a DHCP server.

37.4.1.1 DHCPv4 Relay Agent Information Format

A DHCP Relay Agent Information option has the following format.

Table 151 DHCP Relay Agent Information Option Format

Code (82)	Length (N)	i1	i2	...	iN

i1, i2 and iN are DHCP relay agent sub-options, which contain additional information about the DHCP client. You need to define at least one sub-option.

37.4.1.2 Sub-Option Format

There are two types of sub-option: “Agent Circuit ID Sub-option” and “Agent Remote ID Sub-option”. They have the following formats.

Table 152 DHCP Relay Agent Circuit ID Sub-option Format

SubOpt Code	Length	Value
1 (1 byte)	N (1 byte)	Slot ID, Port ID, VLAN ID, System Name or String

Table 153 DHCP Relay Agent Remote ID Sub-option Format

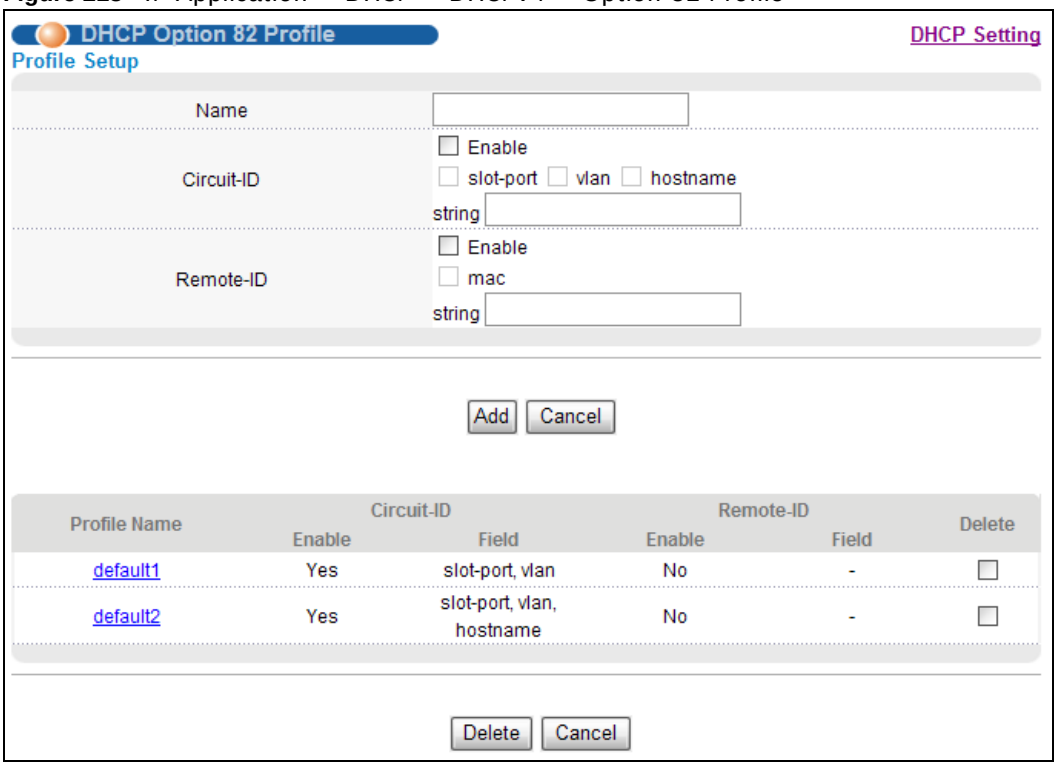
SubOpt Code	Length	Value
2 (1 byte)	N (1 byte)	MAC Address or String

The 1 in the first field identifies this as an Agent Circuit ID sub-option and 2 identifies this as an Agent Remote ID sub-option. The next field specifies the length of the field.

37.4.2 DHCPv4 Option 82 Profile

Use this screen to create DHCPv4 option 82 profiles. Click **IP Application > DHCP > DHCPv4** in the navigation panel and click the **Option 82 Profile** link to display the screen as shown.

Figure 213 IP Application > DHCP > DHCPv4 > Option 82 Profile



The following table describes the labels in this screen.

Table 154 IP Application > DHCP > DHCPv4 > Option 82 Profile

LABEL	DESCRIPTION
Name	Enter a descriptive name for the profile for identification purposes. You can use up to 32 ASCII characters. Spaces are allowed.
Circuit-ID	Use this section to configure the Circuit ID sub-option to include information that is specific to the relay agent (the Switch).
Enable	Select this option to have the Switch add the Circuit ID sub-option to client DHCP requests that it relays to a DHCP server.
slot-port	Select this option to have the Switch add the number of port that the DHCP client is connected to.
vlan	Select this option to have the Switch add the ID of VLAN which the port belongs to.
hostname	This is the system name you configure in the **Basic Setting** > **General Setup** screen. Select this option for the Switch to add the system name to the client DHCP requests that it relays to a DHCP server.
string	Enter a string of up to 64 ASCII characters that the Switch adds into the client DHCP requests. Spaces are allowed.
Remote-ID	Use this section to configure the Remote ID sub-option to include information that identifies the relay agent (the Switch).
Enable	Select this option to have the Switch append the Remote ID sub-option to the option 82 field of DHCP requests.
mac	Select this option to have the Switch add its MAC address to the client DHCP requests that it relays to a DHCP server.
string	Enter a string of up to 64 ASCII characters for the remote ID information in this field. Spaces are allowed.

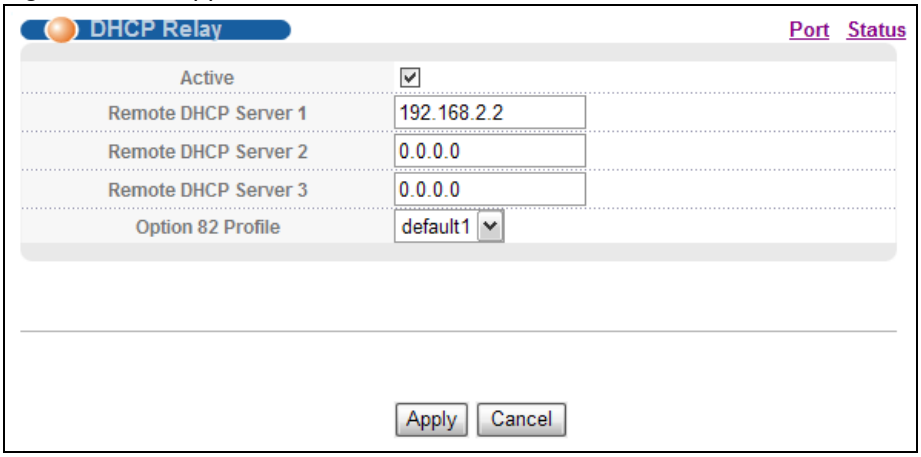
Table 154 IP Application > DHCP > DHCPv4 > Option 82 Profile (continued)

LABEL	DESCRIPTION
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to their last saved values.
Profile Name	This field displays the descriptive name of the profile. Click the name to change the settings.
Circuit-ID	
Enable	This field displays whether the Circuit ID sub-option is added to client DHCP requests.
Field	This field displays the information that is included in the Circuit ID sub-option.
Remote-ID	
Enable	This field displays whether the Remote ID sub-option is added to client DHCP requests.
Field	This field displays the information that is included in the Remote ID sub-option.
Delete	Check the entry(ies) that you want to remove in the **Delete** column and then click the **Delete** button.
Cancel	Click **Cancel** to clear the selected check box(es) in the **Delete** column.

37.4.3 Configuring DHCPv4 Global Relay

Use this screen to configure global DHCPv4 relay. Click **IP Application > DHCP > DHCPv4** in the navigation panel and click the **Global** link to display the screen as shown.

Figure 214 IP Application > DHCP > DHCPv4 > Global



The following table describes the labels in this screen.

Table 155 IP Application > DHCP > DHCPv4 > Global

LABEL	DESCRIPTION
Active	Select this check box to enable DHCPv4 relay.
Remote DHCP Server 1 .. 3	Enter the IP address of a DHCPv4 server in dotted decimal notation.
Option 82 Profile	Select a pre-defined DHCPv4 option 82 profile that the Switch applies to all ports. The Switch adds the Circuit ID sub-option and/or Remote ID sub-option specified in the profile to DHCP requests that it relays to a DHCP server.

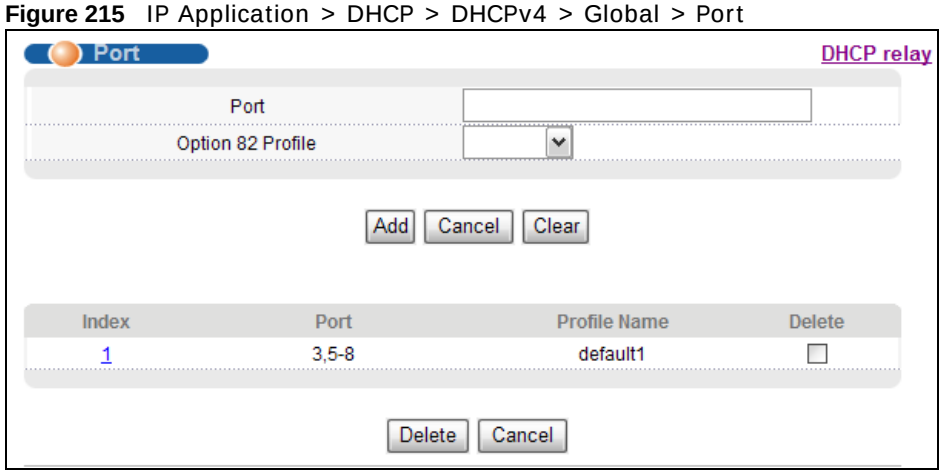
Table 155 IP Application > DHCP > DHCPv4 > Global (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

37.4.4 DHCPv4 Global Relay Port Configure

Use this screen to apply a different DHCP option 82 profile to certain ports on the Switch. To open this screen, click **IP Application > DHCP > DHCPv4 > Global > Port**.

Figure 215 IP Application > DHCP > DHCPv4 > Global > Port



The following table describes the labels in this screen.

Table 156 IP Application > DHCP > DHCPv4 > Global > Port

LABEL	DESCRIPTION
Port	Enter the number of port(s) to which you want to apply the specified DHCP option 82 profile. You can enter multiple ports separated by (no space) comma (,) or hyphen (-). For example, enter "3-5" for ports 3, 4, and 5. Enter "3,5,7" for ports 3, 5, and 7.
Option 82 Profile	Select a pre-defined DHCP option 82 profile that the Switch applies to the specified port(s). The Switch adds the Circuit ID sub-option and/or Remote ID sub-option specified in the profile to DHCP requests that it relays to a DHCP server. The profile you select here has priority over the one you select in the **DHCP > DHCPv4 > Global** screen.
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values above based on the last selected entry or, if not applicable, to clear the fields above.
Clear	Click **Clear** to reset the fields to the factory defaults.
Index	This field displays a sequential number for each entry. Click an index number to change the settings.
Port	This field displays the port(s) to which the Switch applies the settings.

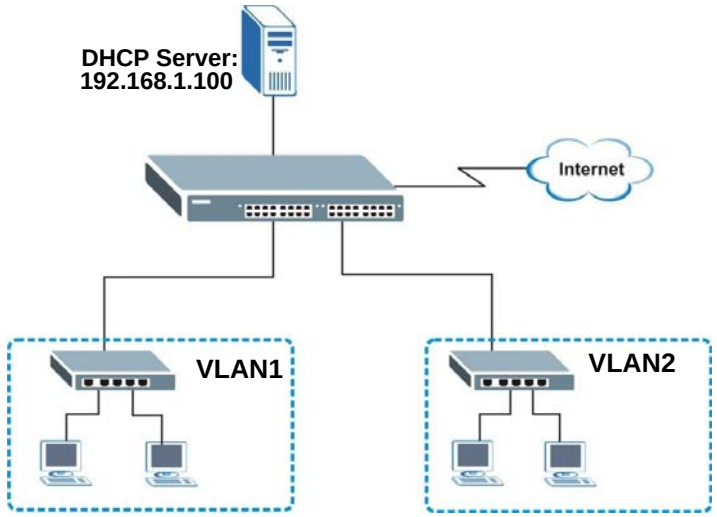
Table 156 IP Application > DHCP > DHCPv4 > Global > Port (continued)

LABEL	DESCRIPTION
Profile Name	This field displays the DHCP option 82 profile that the Switch applies to the port(s).
Delete	Select the entry(ies) that you want to remove in the **Delete** column, then click the **Delete** button to remove the selected entry(ies) from the table.
Delete	Click this to remove selected entry(ies) from the table.
Cancel	Click this to clear the **Delete** check boxes above.

37.4.5 Global DHCP Relay Configuration Example

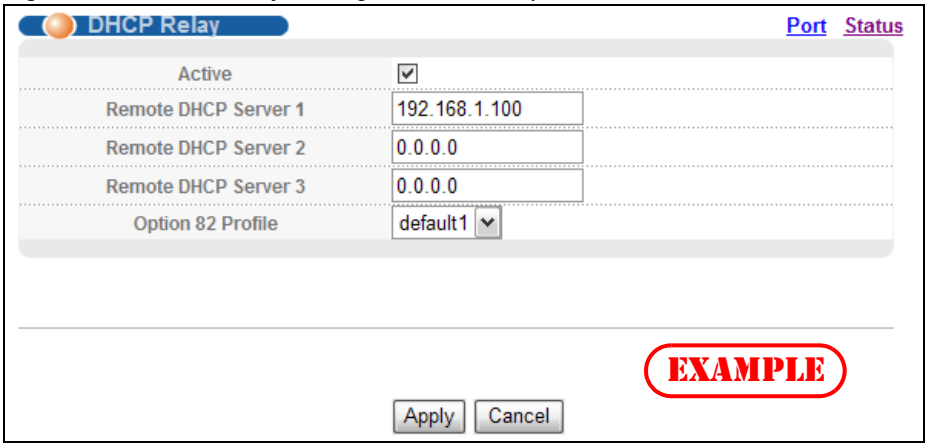
The follow figure shows a network example where the Switch is used to relay DHCP requests for the **VLAN1** and **VLAN2** domains. There is only one DHCP server that services the DHCP clients in both domains.

Figure 216 Global DHCP Relay Network Example



Configure the **DHCP Relay** screen as shown. Make sure you select a DHCP option 82 profile (**default1** in this example) to set the Switch to send additional information (such as the VLAN ID) together with the DHCP requests to the DHCP server. This allows the DHCP server to assign the appropriate IP address according to the VLAN ID.

Figure 217 DHCP Relay Configuration Example

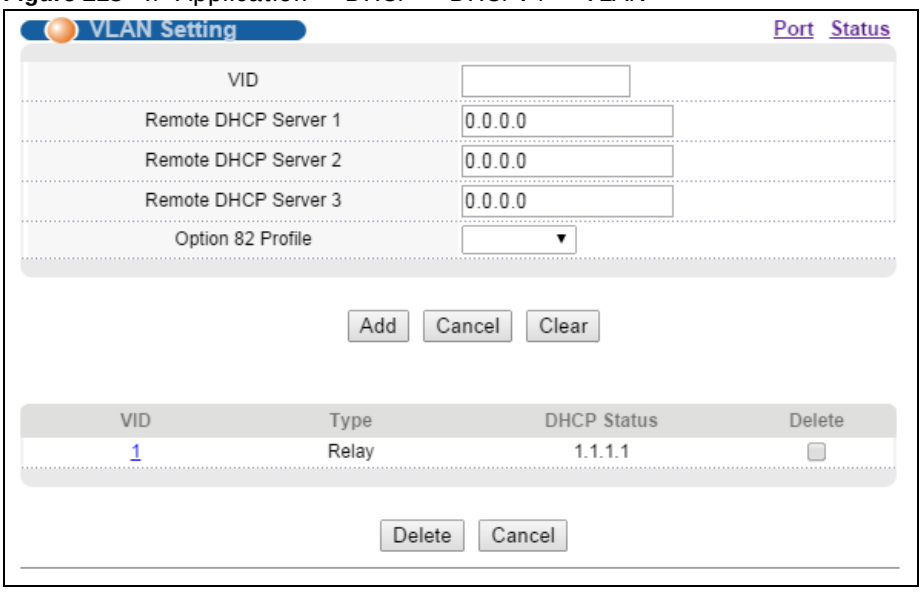


37.5 Configuring DHCPv4 VLAN Settings

Use this screen to configure your DHCP settings based on the VLAN domain of the DHCP clients. Click **IP Application** > **DHCP > DHCPv4** in the navigation panel, then click the **VLAN** link In the **DHCP Status** screen that displays.

Note: You must set up a management IP address for each VLAN that you want to configure DHCP settings for on the Switch.

Figure 218 IP Application > DHCP > DHCPv4 > VLAN



The following table describes the labels in this screen.

Table 157 IP Application > DHCP > DHCPv4 > VLAN

LABEL	DESCRIPTION
VID	Enter the ID number of the VLAN to which these DHCP settings apply.
Remote DHCP Server 1 .. 3	Enter the IP address of a DHCP server in dotted decimal notation.
Option 82 Profile	Select a pre-defined DHCP option 82 profile that the Switch applies to all ports in this VLAN. The Switch adds the Circuit ID sub-option and/or Remote ID sub-option specified in the profile to DHCP requests that it relays to a DHCP server.
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to reset the fields to the factory defaults.
VID	This field displays the ID number of the VLAN group to which this DHCP settings apply.
Type	This field displays **Relay** for the DHCP mode.
DHCP Status	For DHCP server configuration, this field displays the starting IP address and the size of the IP address pool. For DHCP relay configuration, this field displays the first remote DHCP server IP address.
Delete	Select the configuration entries you want to remove and click **Delete** to remove them.

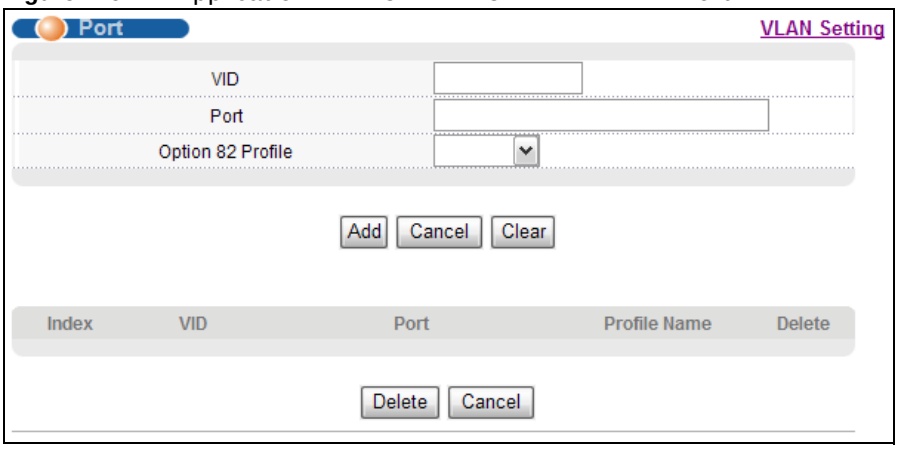
Table 157 IP Application > DHCP > DHCPv4 > VLAN (continued)

LABEL	DESCRIPTION
Delete	Click this to delete selected entries.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

37.5.1 DHCPv4 VLAN Port Configure

Use this screen to apply a different DHCP option 82 profile to certain ports in a VLAN. To open this screen, click **IP Application > DHCP > DHCPv4 > VLAN > Port**.

Figure 219 IP Application > DHCP > DHCPv4 > VLAN > Port



The following table describes the labels in this screen.

Table 158 IP Application > DHCP > DHCPv4 > VLAN > Port

LABEL	DESCRIPTION
VID	Enter the ID number of the VLAN you want to configure here.
Port	Enter the number of port(s) to which you want to apply the specified DHCP option 82 profile. You can enter multiple ports separated by (no space) comma (,) or hyphen (-). For example, enter “3-5” for ports 3, 4, and 5. Enter “3,5,7” for ports 3, 5, and 7.
Option 82 Profile	Select a pre-defined DHCP option 82 profile that the Switch applies to the specified port(s) in this VLAN. The Switch adds the Circuit ID sub-option and/or Remote ID sub-option specified in the profile to DHCP requests that it relays to a DHCP server. The profile you select here has priority over the one you select in the **DHCP > DHCPv4 > VLAN** screen.
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch’s run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values above based on the last selected entry or, if not applicable, to clear the fields above.
Clear	Click **Clear** to reset the fields to the factory defaults.
Index	This field displays a sequential number for each entry. Click an index number to change the settings.
VID	This field displays the VLAN to which the port(s) belongs.

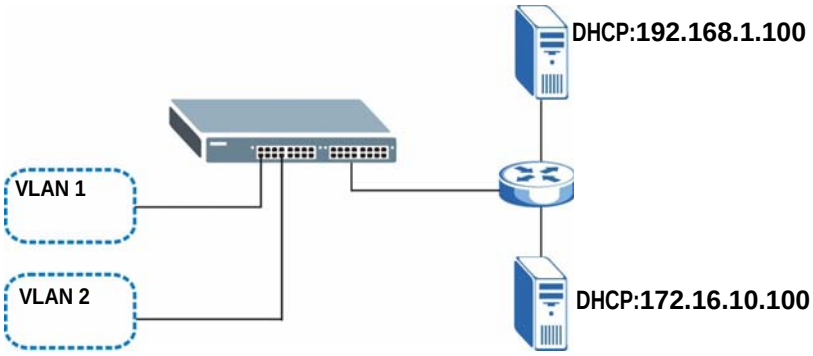
Table 158 IP Application > DHCP > DHCPv4 > VLAN > Port (continued)

LABEL	DESCRIPTION
Port	This field displays the port(s) to which the Switch applies the settings.
Profile Name	This field displays the DHCP option 82 profile that the Switch applies to the port(s) in this VLAN.
Delete	Select the entry(ies) that you want to remove in the **Delete** column, then click the **Delete** button to remove the selected entry(ies) from the table.
Cancel	Click this to clear the **Delete** check boxes above.

37.5.2 Example: DHCP Relay for Two VLANs

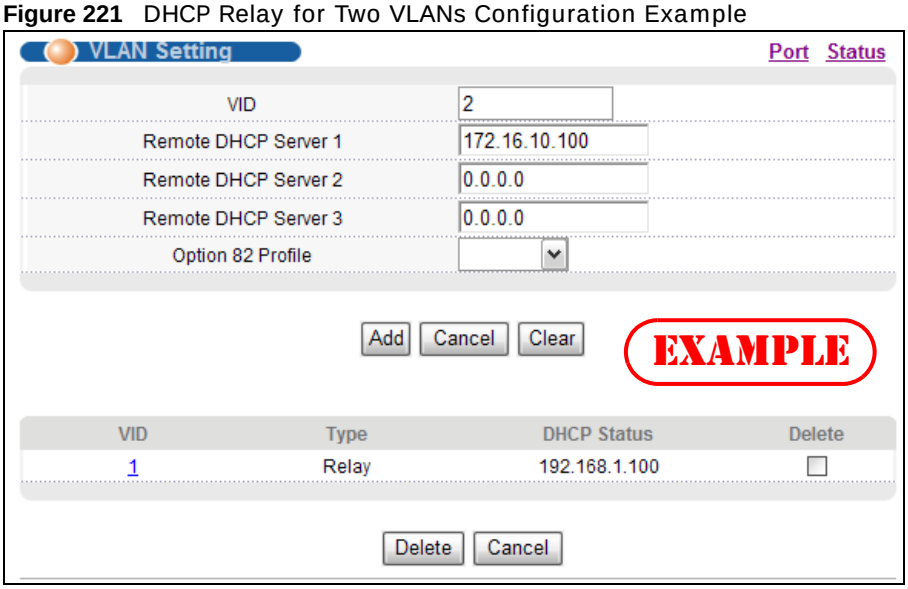
The following example displays two VLANs (VIDs 1 and 2) for a campus network. Two DHCP servers are installed to serve each VLAN. The system is set up to forward DHCP requests from the dormitory rooms (VLAN 1) to the DHCP server with an IP address of 192.168.1.100. Requests from the academic buildings (VLAN 2) are sent to the other DHCP server with an IP address of 172.16.10.100.

Figure 220 DHCP Relay for Two VLANs



For the example network, configure the **VLAN Setting** screen as shown.

Figure 221 DHCP Relay for Two VLANs Configuration Example



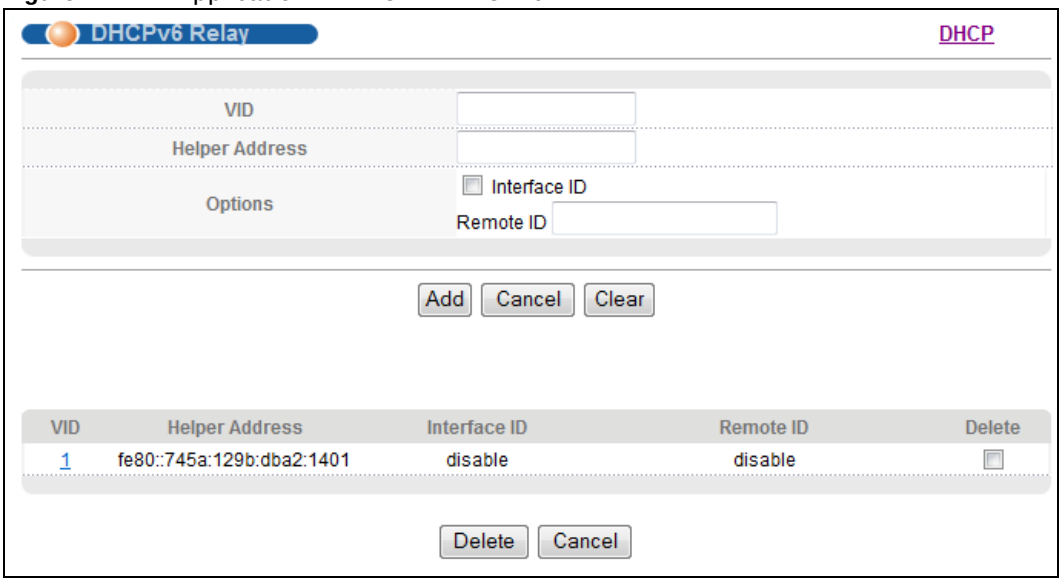
37.6 DHCPv6 Relay

A DHCPv6 relay agent is on the same network as the DHCPv6 clients and helps forward messages between the DHCPv6 server and clients. When a client cannot use its link-local address and a well-known multicast address to locate a DHCPv6 server on its network, it then needs a DHCPv6 relay agent to send a message to a DHCPv6 server that is not attached to the same network.

The DHCPv6 relay agent can add the remote identification (remote-ID) option and the interface-ID option to the Relay-Forward DHCPv6 messages. The remote-ID option carries a user-defined string, such as the system name. The interface-ID option provides slot number, port information and the VLAN ID to the DHCPv6 server. The remote-ID option (if any) is stripped from the Relay-Reply messages before the relay agent sends the packets to the clients. The DHCPv6 server copies the interface-ID option from the Relay-Forward message into the Relay-Reply message and sends it to the relay agent. The interface-ID should not change even after the relay agent restarts.

Use this screen to configure DHCPv6 relay settings for a specific VLAN on the Switch. Click **IP Application > DHCP > DHCPv6** in the navigation panel to display the screen as shown.

Figure 222 IP Application > DHCP > DHCPv6



The following table describes the labels in this screen.

Table 159 IP Application > DHCP > DHCPv6

LABEL	DESCRIPTION
VID	Enter the ID number of the VLAN you want to configure here.
Helper Address	Enter the remote DHCPv6 server address for the specified VLAN.
Options	
Interface ID	Select this option to have the Switch add the interface-ID option in the DHCPv6 requests from the clients in the specified VLAN before the Switch forwards them to a DHCPv6 server.
Remote ID	Enter a string of up to 64 printable characters to be carried in the remote-ID option. The Switch adds the remote-ID option in the DHCPv6 requests from the clients in the specified VLAN before the Switch forwards them to a DHCPv6 server.

Table 159 IP Application > DHCP > DHCPv6 (continued)

LABEL	DESCRIPTION
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to their last saved values.
Clear	Click **Clear** to reset the fields to the factory defaults.
VID	This field displays the VLAN ID number. Click the VLAN ID to change the settings.
Helper Address	This field displays the IPv6 address of the remote DHCPv6 server for this VLAN.
Interface ID	This field displays whether the interface-ID option is added to DHCPv6 requests from clients in this VLAN.
Remote ID	This field displays whether the remote-ID option is added to DHCPv6 requests from clients in this VLAN.
Delete	Check the entry(ies) that you want to remove in the **Delete** column and then click the **Delete** button.
Cancel	Click **Cancel** to clear the selected check box(es) in the **Delete** column.

38

ARP Setup

38.1 ARP Overview

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control or MAC address, on the local area network.

An IP (version 4) address is 32 bits long. In an Ethernet LAN, MAC addresses are 48 bits long. The ARP table maintains an association between each MAC address and its corresponding IP address.

- Use the **ARP Learning** screen (Section 38.2.1 on page 315) to configure ARP learning mode on a per-port basis.
- Use the **Static ARP** screen to create static ARP entries that will display in the **Management > ARP Table** screen and will not age out.

38.1.1 How ARP Works

When an incoming packet destined for a host device on a local area network arrives at the Switch, the Switch looks in the ARP Table and if it finds the address, it sends it to the device.

If no entry is found for the IP address, ARP broadcasts the request to all the devices on the LAN. The Switch fills in its own MAC and IP address in the sender address fields, and puts the known IP address of the target in the target IP address field. In addition, the Switch puts all ones in the target MAC field (FF.FF.FF.FF.FF.FF is the Ethernet broadcast address). The replying device (which is either the IP address of the device being sought or the router that knows the way) replaces the broadcast address with the target's MAC address, swaps the sender and target pairs, and unicasts the answer directly back to the requesting machine. ARP updates the ARP Table for future reference and then sends the packet to the MAC address that replied.

38.1.2 ARP Learning Mode

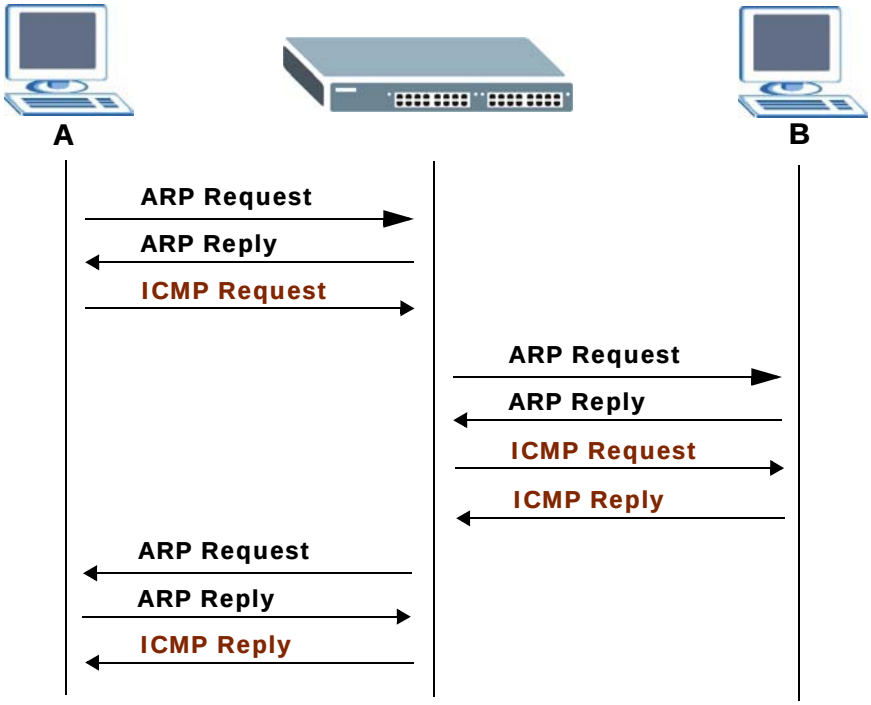
The Switch supports three ARP learning modes: ARP-Reply, Gratuitous-ARP, and ARP-Request.

38.1.2.1 ARP-Reply

By default, the Switch is in ARP-Reply learning mode and updates the ARP table only with the ARP replies to the ARP requests sent by the Switch. This can help prevent ARP spoofing.

In the following example, the Switch does not have IP address and MAC address mapping information for hosts **A** and **B** in its ARP table, and host **A** wants to ping host **B**. Host **A** sends an ARP request to the Switch and then sends an ICMP request after getting the ARP reply from the Switch. The Switch finds no matched entry for host **B** in the ARP table and broadcasts the ARP request to all the devices on the LAN. When the Switch receives the ARP reply from host **B**, it updates its ARP table and also forwards host **A**'s ICMP request to host **B**. After the Switch gets the

ICMP reply from host **B**, it sends out an ARP request to get host **A**'s MAC address and updates the ARP table with host **A**'s ARP reply. The Switch then can forward host **B**'s ICMP reply to host **A**.



38.1.2.2 Gratuitous-ARP

A gratuitous ARP is an ARP request in which both the source and destination IP address fields are set to the IP address of the device that sends this request and the destination MAC address field is set to the broadcast address. There will be no reply to a gratuitous ARP request.

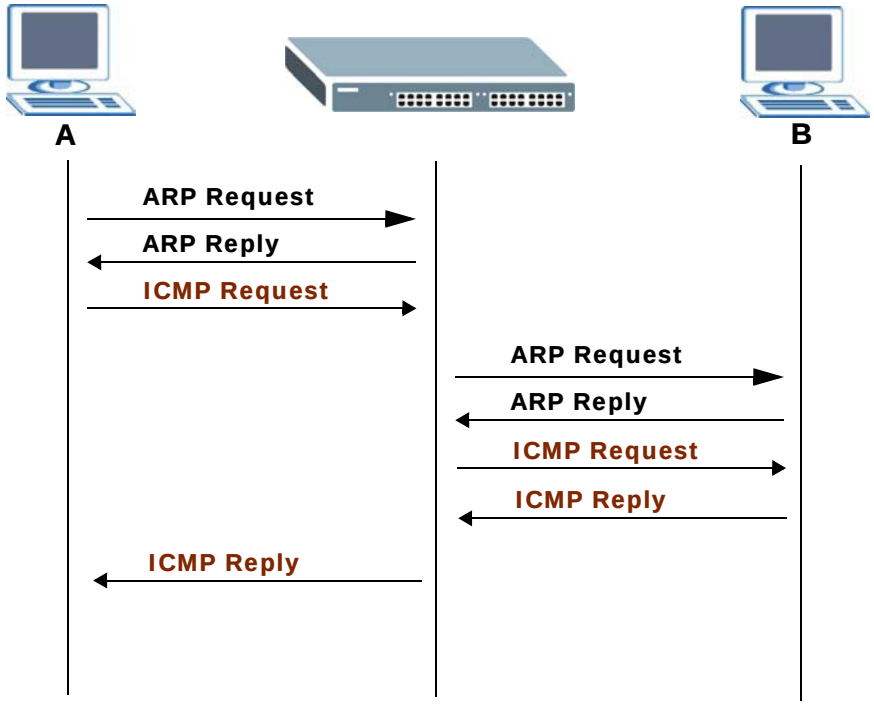
A device may send a gratuitous ARP packet to detect IP collisions. If a device restarts or its MAC address is changed, it can also use gratuitous ARP to inform other devices in the same network to update their ARP table with the new mapping information.

In Gratuitous-ARP learning mode, the Switch updates its ARP table with either an ARP reply or a gratuitous ARP request.

38.1.2.3 ARP-Request

When the Switch is in ARP-Request learning mode, it updates the ARP table with both ARP replies, gratuitous ARP requests and ARP requests.

Therefore in the following example, the Switch can learn host **A**'s MAC address from the ARP request sent by host **A**. The Switch then forwards host **B**'s ICMP reply to host **A** right after getting host **B**'s MAC address and ICMP reply.



38.2 ARP Setup

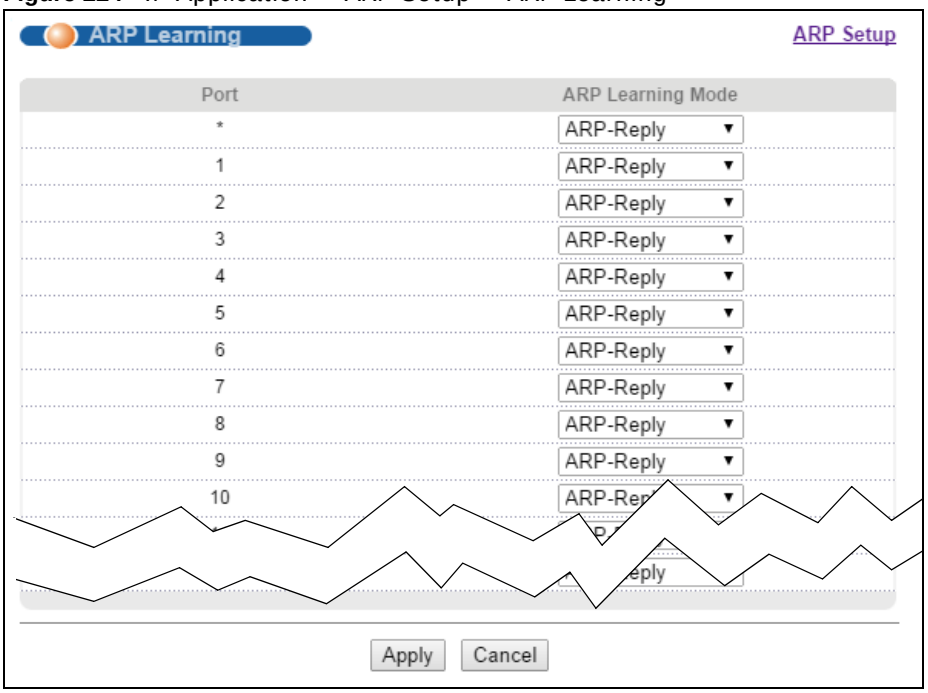
Click **IP Application** > **ARP Setup** in the navigation panel to display the screen as shown. Click the link next to **ARP Learning** to open a screen where you can set the ARP learning mode for each port. Click the link next to **Static ARP** to open a screen where you can create static ARP entries on the Switch.

Figure 223 IP Application > ARP Setup

38.2.1 ARP Learning

Use this screen to configure each port's ARP learning mode. Click the link next to **ARP Learning** in the **IP Application** > **ARP Setup** screen to display the screen as shown next.

Figure 224 IP Application > ARP Setup > ARP Learning



The following table describes the labels in this screen.

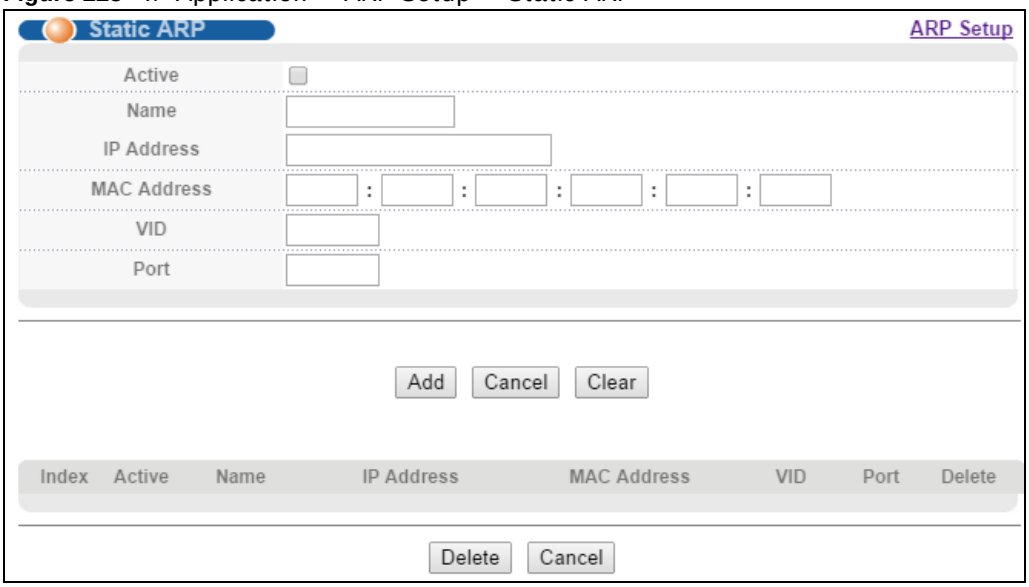
Table 160 IP Application > ARP Setup > ARP Learning

LABEL	DESCRIPTION
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Changes in this row are copied to all the ports as soon as you make them.
ARP Learning Mode	Select the ARP learning mode the Switch uses on the port. Select **ARP-Reply** to have the Switch update the ARP table only with the ARP replies to the ARP requests sent by the Switch. Select **Gratuitous-ARP** to have the Switch update its ARP table with either an ARP reply or a gratuitous ARP request. Select **ARP-Request** to have the Switch update the ARP table with both ARP replies, gratuitous ARP requests and ARP requests.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

38.2.2 Static ARP

Use this screen to create static ARP entries that will display in the **Management > ARP Table** screen and will not age out. Click the link next to **Static ARP** in the **IP Application** > **ARP Setup** screen to display the screen as shown.

Figure 225 IP Application > ARP Setup > Static ARP



The following table describes the related labels in this screen.

Table 161 IP Application > ARP Setup > Static ARP

LABEL	DESCRIPTION
Active	Select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by clearing this check box.
Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.
IP Address	Enter the IP address of a device connected to a Switch port with the corresponding MAC address below.
MAC Address	Enter the MAC address of the device with the corresponding IP address above.
VID	Enter the ID number of VLAN to which the device belongs.
Port	Enter the number of port to which the device connects.
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to set the above fields back to the factory defaults.
Index	This field displays the index number of an entry. Click an index number to change the settings.
Active	This field displays **Yes** when the entry is activated and **NO** when it is deactivated.
Name	This field displays the descriptive name for this entry. This is for identification purposes only.
IP Address	This is the IP address of a device connected to a Switch port with the corresponding MAC address below.
MAC Address	This is the MAC address of the device with the corresponding IP address above.
VID	This field displays the VLAN to which the device belongs.
Port	This field displays the port to which the device connects.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

39

Maintenance

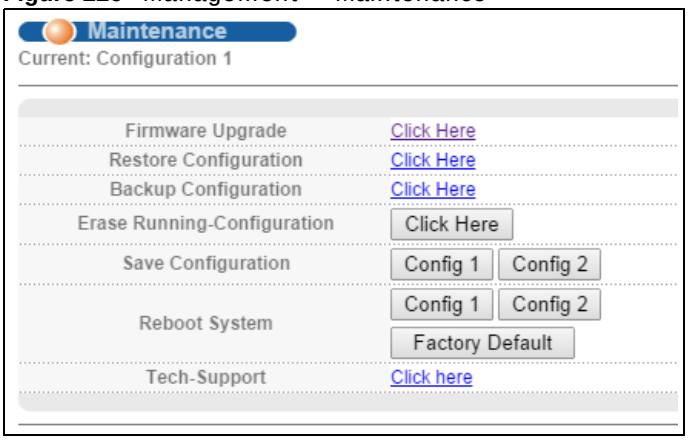
39.1 Overview

This chapter explains how to configure the screens that let you maintain the firmware and configuration files.

39.2 The Maintenance Screen

Use this screen to manage firmware and your configuration files. Click **Management** > **Maintenance** in the navigation panel to open the following screen.

Figure 226 Management > Maintenance



The following table describes the labels in this screen.

Table 162 Management > Maintenance

LABEL	DESCRIPTION
Current	This field displays which configuration (**Configuration 1** or **Configuration 2**) is currently operating on the Switch.
Firmware Upgrade	Click **Click Here** to go to the **Firmware Upgrade** screen.
Restore Configuration	Click **Click Here** to go to the **Restore Configuration** screen.
Backup Configuration	Click **Click Here** to go to the **Backup Configuration** screen.
Erase Running-Configuration	Click **Click Here** to reset the current configuration of the Switch. Note that this will not reset the configuration to the factory default settings.

Table 162 Management > Maintenance (continued)

LABEL	DESCRIPTION
Save Configuration	Click **Config 1** to save the current configuration settings to **Configuration 1** on the Switch. Click **Config 2** to save the current configuration settings to **Configuration 2** on the Switch.
Reboot System	Click **Config 1** to reboot the system and load **Configuration 1** on the Switch. Click **Config 2** to reboot the system and load **Configuration 2** on the Switch. Note: Make sure to click the **Save** button in any screen to save your settings to the current configuration on the Switch.
Factory Default	Click this to reset the Switch IP address, admin username and password, and other configuration settings back to the factory defaults.
Tech Support	Click **Click Here** to see the Tech-Support screen. You can set CPU and memory thresholds for log reports and download related log reports for issue analysis. Log reports include CPU history and utilization, crash and memory.

39.2.1 Firmware Upgrade

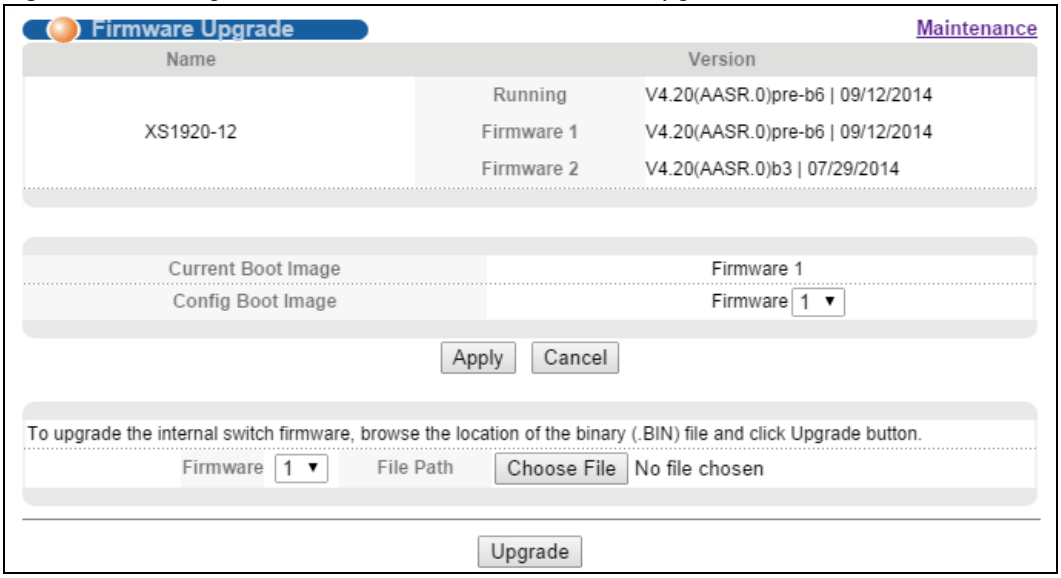
Use the following screen to upgrade your Switch to the latest firmware. The Switch supports dual firmware images, **Firmware 1** and **Firmware 2**. Use this screen to specify which image is updated when firmware is uploaded using the web configurator and to specify which image is loaded when the Switch starts up.

Make sure you have downloaded (and unzipped) the correct model firmware and version to your computer before uploading to the device.

Be sure to upload the correct model firmware as uploading the wrong model firmware may damage your device.

Click **Management** > **Maintenance** > **Firmware Upgrade** to view the screen as shown next.

Figure 227 Management > Maintenance > Firmware Upgrade



The top of firmware upgrade screen shows which firmware version is currently running on the Switch. Select the **Config Boot Image** drop-down list box if you want to reboot the Switch and click **Apply** to apply the new firmware immediately. (Firmware upgrades are only applied after a reboot). Click **Upgrade** to load the new firmware. After the firmware upgrade process is complete, see the **System Info** screen to verify your current firmware version number.

The following table describes the labels in this screen.

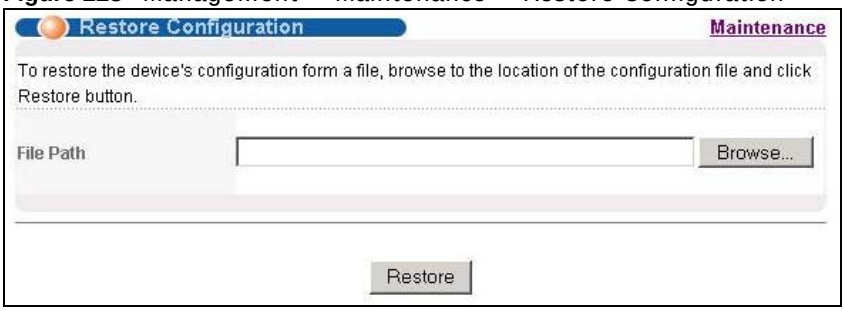
Table 163 Management > Maintenance> Firmware Upgrade

LABEL	DESCRIPTION
Name	This is the name of the Switch that you're configuring.
Version	The Switch has two firmware sets, **Firmware 1** and **Firmware 2**, residing in flash. • **Running** shows the version number (and model code) and MM/DD/YYYY creation date of the firmware currently in use on the Switch (**Firmware 1** or **Firmware 2)**. The firmware information is also displayed at System Information in Basic Settings. • **Firmware 1** shows its version number (and model code) and MM/DD/YYYY creation date. • **Firmware 2** shows its version number (and model code) and MM/DD/YYYY creation date.
Current Boot Image	This displays which firmware is currently in use on the Switch (**Firmware 1** or **Firmware 2)**.
Config Boot Image	Select which firmware (**Firmware 1** or **Firmware 2)** should load, click Apply and reboot the switch to see changes, you will also see changes in the Current boot image field above as well.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Firmware	Choose to upload the new firmware to (Firmware) **1** or (Firmware) **2**.
File Path	Type the path and file name of the firmware file you wish to upload to the Switch in the **File Path** text box or click **Browse** to locate it.
Upgrade	Click **Upgrade** to load the new firmware. Firmware upgrades are only applied after a reboot. To reboot, go to **Management > Maintenance > Reboot System** and click **Config 1** or **Config 2** to select which configuration file to upload after reboot.

39.2.2 Restore a Configuration File

Use this screen to restore a previously saved configuration from your computer to the Switch using the **Restore Configuration** screen.

Figure 228 Management > Maintenance > Restore Configuration


Restore Configuration
Maintenance
To restore the device's configuration form a file, browse to the location of the configuration file and click Restore button.
File Path
Browse...
Restore

Type the path and file name of the configuration file you wish to restore in the **File Path** text box or click **Browse** to locate it. After you have specified the file, click **Restore**. "config" is the name of

the configuration file on the Switch, so your backup configuration file is automatically renamed when you restore using this screen.

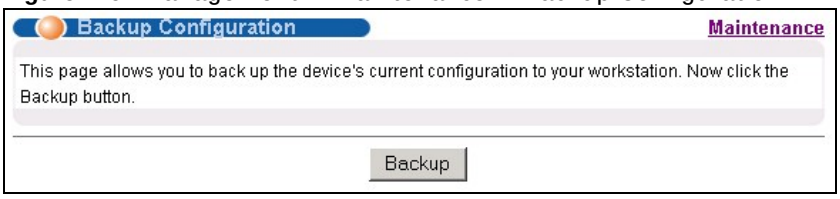
39.2.3 Backup a Configuration File

Use this screen to save and store your current device settings.

Backing up your Switch configurations allows you to create various “snap shots” of your device from which you may restore at a later date.

Back up your current Switch configuration to a computer using the **Backup Configuration** screen.

Figure 229 Management > Maintenance > Backup Configuration


Backup Configuration
Maintenance
This page allows you to back up the device's current configuration to your workstation. Now click the Backup button.
Backup

Follow the steps below to back up the current Switch configuration to your computer in this screen.

1 Click **Backup**.

2 Click **Save** to display the **Save As** screen.

3 Choose a location to save the file on your computer from the **Save in** drop-down list box and type a descriptive name for it in the **File name** list box. Click **Save** to save the configuration file to your computer.

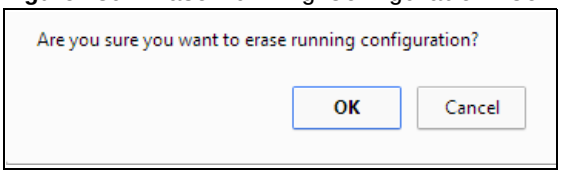
39.2.4 Erase Running-Configuration

Follow the steps below to clear current configuration on the Switch. Note that this will NOT reset the Switch back to its factory defaults. If you want to change the Switch to its factory default mode, click Factory Default button in Reboot System. See (Section 39.2.1 on page 319).

1 In the **Maintenance** screen, click the **Click Here** button next to **Erase Running-Configuration** to clear all Switch configuration information you configured on the Switch.

2 Click **OK** to reset all Switch configurations.

Figure 230 Erase Running-Configuration: Confirmation



3 In the web configurator, click the **Save** button in the top of the screen to make the changes take effect. If you want to access the Switch web configurator again, you may need to change the IP address of your computer to be in the same subnet as that of the default Switch IP address (192.168.1.1).

39.2.5 Save Configuration

Click **Config 1** to save the current configuration settings permanently to **Configuration 1** on the Switch.

Click **Config 2** to save the current configuration settings to **Configuration 2** on the Switch.

Alternatively, click Save on the top right-hand corner in any screen to save the configuration changes to the current configuration.

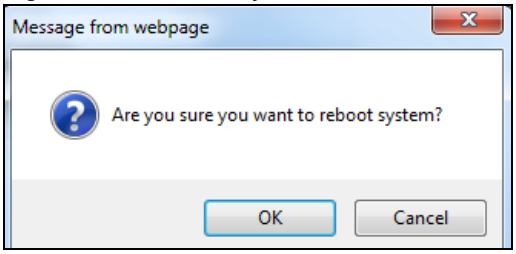
Note: Clicking the **Apply** or **Add** button does NOT save the changes permanently. All unsaved changes are erased after you reboot the Switch.

39.2.6 Reboot System

Reboot System allows you to restart the Switch without physically turning the power off. It also allows you to load configuration one (**Config 1**) or configuration two (**Config 2**) when you reboot. Follow the steps below to reboot the Switch.

1 In the **Maintenance** screen, click the **Config 1** button next to **Reboot System** to reboot and load configuration one. The following screen displays.

Figure 231 Reboot System: Confirmation



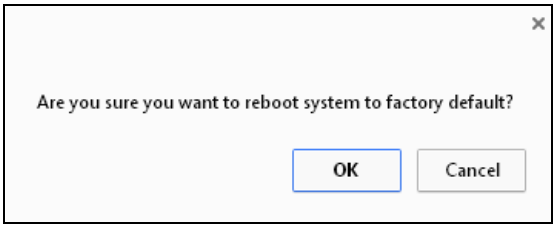
2 Click **OK** again and then wait for the Switch to restart. This takes up to two minutes. This does not affect the Switch's configuration.

Click **Config 2** and follow steps 1 to 2 to reboot and load configuration two on the Switch.

39.2.7 Factory Default

Follow the steps below to reset the Switch back to the factory defaults using the web configurator. See Section 3.4 on page 29 to reset the Switch using the **Reset** button. It is recommended to back up your current configuration before resetting.

1 In the **Maintenance** screen, click the **Factory Default** button to clear all Switch configuration information you configured and return to the factory defaults.

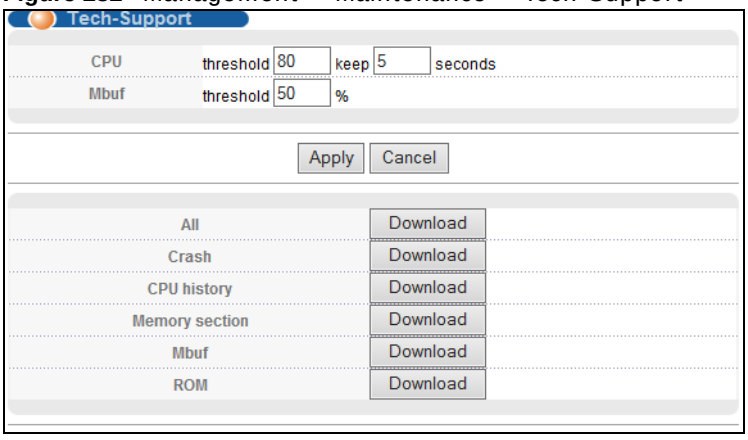


2 Click **OK** to reset all Switch configurations to the factory defaults.

39.3 Tech-Support

The Tech-Support feature is a log enhancement tool that logs useful information such as CPU utilization history, memory and Mbuf (Memory Buffer) log and crash reports for issue analysis by customer support should you have difficulty with your Switch. Click **Menu** > **Management** > **Maintenance** > **Tech-Support** to see the following screen.

Figure 232 Management > Maintenance > Tech-Support



You may need WordPad or similar software to see the log report correctly. The table below describes the fields in the above screen.

Table 164 Management > Maintenance > Tech-Support

CPU	Type a number ranging from 50 to 100 in the CPU threshold box, and type another number ranging from 5 to 60 in the seconds box then click **Apply**. For example, 80 for CPU threshold and 5 for seconds means a log will be created when CPU utilization reaches over 80% and lasts for 5 seconds. The log report holds 7 days of CPU log data and is stored in volatile memory (RAM). The data is lost if the Switch is turned off or in event of power outage. After 7 days, the logs wrap around and new ones and replace the earliest ones. The higher the CPU threshold number, the fewer logs will be created, and the less data technical support will have to analyze and vice versa.
Mbuf	Type a number ranging from 50 to 100 in the Mbuf (Memory Buffer) threshold box. The Mbuf log report is stored in flash (permanent) memory. For example, Mbuf 50 means a log will be created when the Mbuf utilization is over 50%. The higher the Mbuf threshold number, the fewer logs will be created, and the less data technical support will have to analyze and vice versa.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

Table 164 Management > Maintenance > Tech-Support

All	Click **Download** to see all the log report and system status. This log report is stored in flash memory. If the **All** log report is too large, you can download the log reports separately below.
Crash	Click **Download** to see the crash log report. The log will include information of the last crash and is stored in flash memory.
CPU history	Click **Download** to see the CPU history log report. The 7-days log is stored in RAM and you will need to save it, otherwise it will be lost when the Switch is shutdown or when there is a power outage.
Memory Section	Click **Download** to see the memory section log report. This log report is stored in flash memory.
Mbuf	Click **Download** to see the Mbuf log report. The log includes Mbuf over threshold information. This log report is stored in flash memory.
ROM	Click **Download** to see the Read Only Memory (ROM) log report. This report is stored in flash memory.

39.4 Technical Reference

This section provides technical background information on the topics discussed in this chapter.

39.4.1 FTP Command Line

This section shows some examples of uploading to or downloading files from the Switch using FTP commands. First, understand the filename conventions.

39.4.2 Filename Conventions

The configuration file (also known as the romfile or ROM) contains the factory default settings in the screens such as password, Switch setup, IP Setup, and so on. Once you have customized the Switch's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS (ZyXEL Network Operating System sometimes referred to as the "ras" file) is the system firmware and has a "bin" filename extension.

Table 165 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	config	*.cfg	This is the configuration filename on the Switch. Uploading the config file replaces the specified configuration file system, including your Switch configurations, system-related data (including the default password), the error log and the trace log.
Firmware	ras-0 (Firmware 1) ras-1 (Firmware 2)	*.bin	This is the generic name for the ZyNOS firmware on the Switch.

39.4.2.1 Example FTP Commands

```
ftp> put firmware.bin ras-0
```

This is a sample FTP session showing the transfer of the computer file "firmware.bin" to the Switch.

```
ftp> get config config.cfg
```

This is a sample FTP session saving the current configuration to a file called “config.cfg” on your computer.

If your (T)FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the Switch only recognizes “config” and “ras”. Be sure you keep unaltered copies of both files for later use.

Be sure to upload the correct model firmware as uploading the wrong model firmware may damage your device.

39.4.3 FTP Command Line Procedure

1. Launch the FTP client on your computer.
2. Enter open, followed by a space and the IP address of your Switch.
3. Press [ENTER] when prompted for a username.
4. Enter your password as requested (the default is “1234”).
5. Enter bin to set transfer mode to binary.
6. Use put to transfer files from the computer to the Switch, for example, `put firmware.bin ras-0` transfers the firmware on your computer (firmware.bin) to the Switch and renames it to “ras-0”. Similarly, `put config.cfg config` transfers the configuration file on your computer (config.cfg) to the Switch and renames it to “config”. Likewise `get config config.cfg` transfers the configuration file on the Switch to your computer and renames it to “config.cfg”. See Table 165 on page 324 for more information on filename conventions.
7. Enter quit to exit the ftp prompt.

39.4.4 GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

Table 166 General Commands for GUI-based FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	Anonymous. This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option. Normal. The server requires a unique User ID and Password to login.
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode. Configuration and firmware files should be transferred in binary mode.

Table 166 General Commands for GUI-based FTP Clients (continued)

COMMAND	DESCRIPTION
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

39.4.5 FTP Restrictions

FTP will not work when:

- FTP service is disabled in the **Service Access Control** screen.
- The IP address(es) in the **Remote Management** screen does not match the client IP address. If it does not match, the Switch will disconnect the FTP session immediately.

40

Access Control

40.1 Access Control Overview

This chapter describes how to control access to the Switch.

One FTP session, up to five Web sessions (five different user names and passwords) and/or limitless SNMP access control sessions are allowed.

Table 167 Access Control Overview

FTP	Web	SNMP
One session	Up to five accounts	No limit

40.1.1 What You Can Do

Use the **Access Control** screen (Section 40.2 on page 327) to display the main screen.

- Use the **SNMP** screen (Section 40.3 on page 328) to configure your SNMP settings.
  - Use the **Trap Group** screen (Section 40.3.1 on page 329) to specify the types of SNMP traps that should be sent to each SNMP manager.
  - Use the **User Information** screen (Section 40.3.3 on page 331) to create SNMP users for authentication with managers using SNMP v3 and associate them to SNMP groups.
- Use the **Logins** screens (Section 40.4 on page 332) to assign which users can access the Switch via web configurator at any one time.
- Use the **Service Access Control** screen (Section 40.5 on page 334) to decide what services you may use to access the Switch.
- Use the **Remote Management** screen (Section 40.6 on page 335) to specify a group of one or more “trusted computers” from which an administrator may use a service to manage the Switch.

40.2 The Access Control Main Screen

Use this screen to display the main screen.

Click **Management** > **Access Control** in the navigation panel to display the main screen as shown.

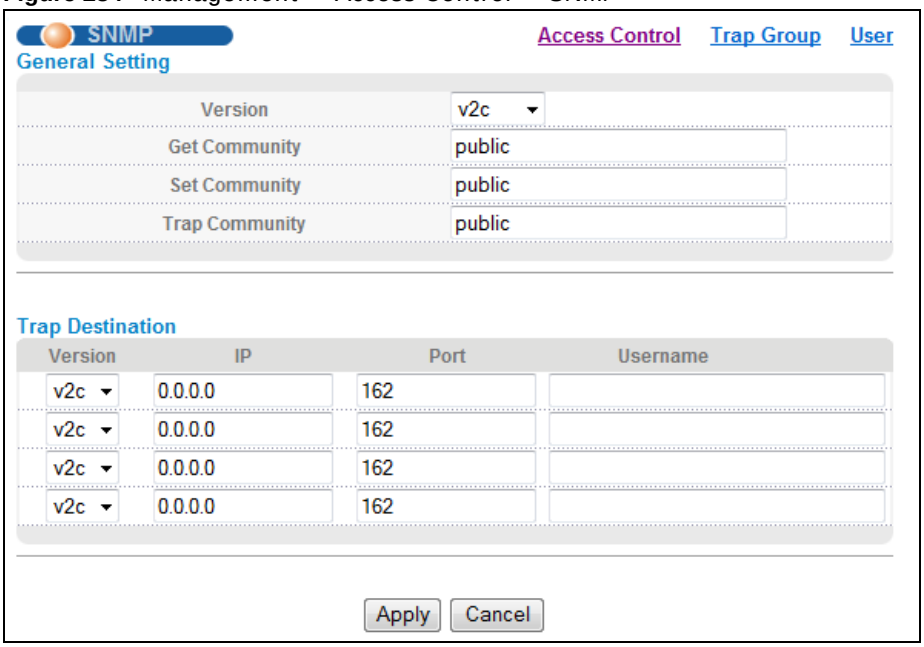
Figure 233 Management > Access Control

40.3 Configuring SNMP

Use this screen to configure your SNMP settings.

Click **Management** > **Access Control** > **SNMP** to view the screen as shown.

Figure 234 Management > Access Control > SNMP



The following table describes the labels in this screen.

Table 168 Management > Access Control > SNMP

LABEL	DESCRIPTION
General Setting	Use this section to specify the SNMP version and community (password) values.
Version	Select the SNMP version for the Switch. The SNMP version on the Switch must match the version on the SNMP manager. Choose SNMP version 2c (**v2c**), SNMP version 3 (**v3**) or both (**v3v2c**). SNMP version 2c is backwards compatible with SNMP version 1.
Get Community	Enter the **Get Community** string, which is the password for the incoming Get- and GetNext- requests from the management station. The **Get Community** string is only used by SNMP managers using SNMP version 2c or lower.

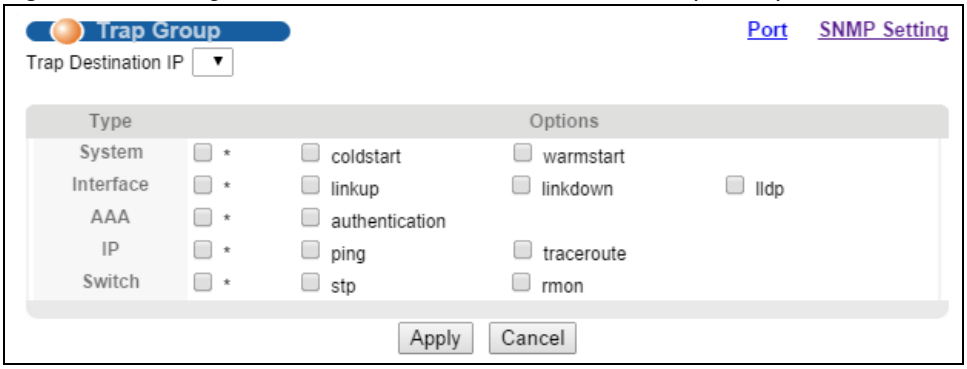
Table 168 Management > Access Control > SNMP (continued)

LABEL	DESCRIPTION
Set Community	Enter the **Set Community**, which is the password for incoming Set- requests from the management station. The **Set Community** string is only used by SNMP managers using SNMP version 2c or lower.
Trap Community	Enter the **Trap Community** string, which is the password sent with each trap to the SNMP manager. The **Trap Community** string is only used by SNMP managers using SNMP version 2c or lower.
Trap Destination	Use this section to configure where to send SNMP traps from the Switch.
Version	Specify the version of the SNMP trap messages.
IP	Enter the IP addresses of up to four managers to send your SNMP traps to.
Port	Enter the port number upon which the manager listens for SNMP traps.
Username	Enter the username to be sent to the SNMP manager along with the SNMP v3 trap. This username must match an existing account on the Switch (configured in **Management** > **Access Control** > **Logins** screen).
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

40.3.1 Configuring SNMP Trap Group

From the **SNMP** screen, click **Trap Group** to view the screen as shown. Use the **Trap Group** screen to specify the types of SNMP traps that should be sent to each SNMP manager.

Figure 235 Management > Access Control > SNMP > Trap Group



The following table describes the labels in this screen.

Table 169 Management > Access Control > SNMP > Trap Group

LABEL	DESCRIPTION
Trap Destination IP	Select one of your configured trap destination IP addresses. These are the IP addresses of the SNMP managers. You must first configure a trap destination IP address in the **SNMP Setting** screen. Use the rest of the screen to select which traps the Switch sends to that SNMP manager.
Type	Select the categories of SNMP traps that the Switch is to send to the SNMP manager.

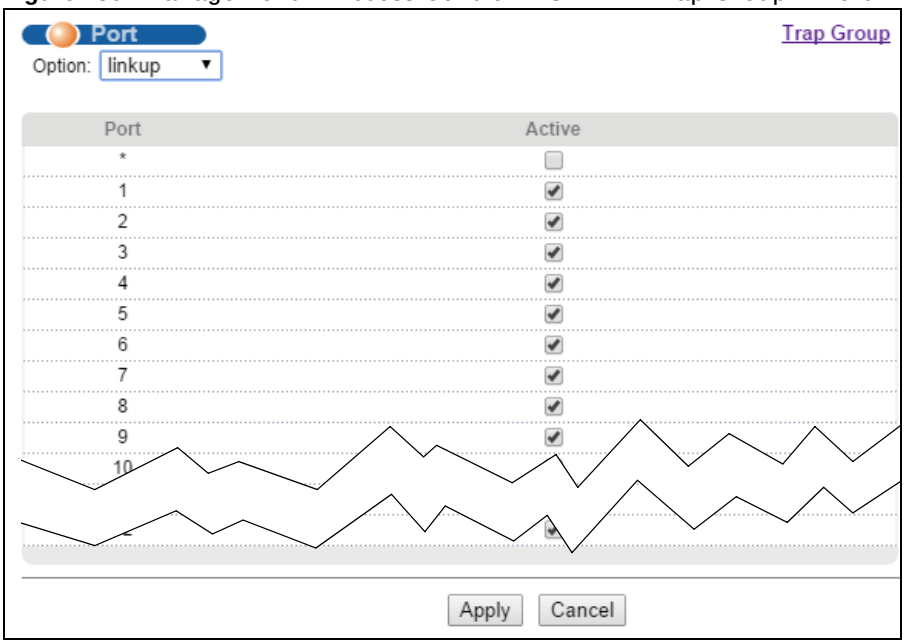
Table 169 Management > Access Control > SNMP > Trap Group (continued) (continued)

LABEL	DESCRIPTION
Options	Select the individual SNMP traps that the Switch is to send to the SNMP station. See SNMP Traps on page 338 for individual trap descriptions. The traps are grouped by category. Selecting a category automatically selects all of the category's traps. Clear the check boxes for individual traps that you do not want the Switch to send to the SNMP station. Clearing a category's check box automatically clears all of the category's trap check boxes (the Switch only sends traps from selected categories).
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

40.3.2 Enabling/Disabling Sending of SNMP Traps on a Port

From the **SNMP > Trap Group** screen, click **Port** to view the screen as shown. Use this screen to set whether a trap received on the port(s) would be sent to the SNMP manager.

Figure 236 Management > Access Control > SNMP > Trap Group > Port



The following table describes the labels in this screen.

Table 170 Management > Access Control > SNMP > Trap Group > Port

LABEL	DESCRIPTION
Option	Select the trap type you want to configure here.
Port	This field displays a port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some of the settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Changes in this row are copied to all the ports as soon as you make them.

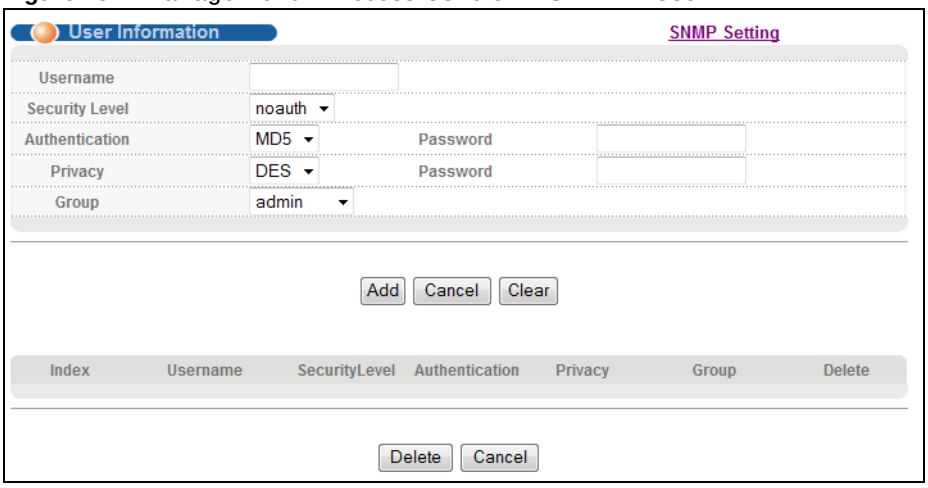
Table 170 Management > Access Control > SNMP > Trap Group > Port (continued)

LABEL	DESCRIPTION
Active	Select this check box to enable the trap type of SNMP traps on this port. Clear this check box to disable the sending of SNMP traps on this port.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

40.3.3 Configuring SNMP User

From the **SNMP** screen, click **User** to view the screen as shown. Use the **User** screen to create SNMP users for authentication with managers using SNMP v3 and associate them to SNMP groups. An SNMP user is an SNMP manager.

Figure 237 Management > Access Control > SNMP > User



The following table describes the labels in this screen.

Table 171 Management > Access Control > SNMP > User

LABEL	DESCRIPTION
User Information	Note: Use the username and password of the login accounts you specify in this screen to create accounts on the SNMP v3 manager.
Username	Specify the username of a login account on the Switch.
Security Level	Select whether you want to implement authentication and/or encryption for SNMP communication from this user. Choose: • noauth -to use the username as the password string to send to the SNMP manager. This is equivalent to the Get, Set and Trap Community in SNMP v2c. This is the lowest security level. • auth - to implement an authentication algorithm for SNMP messages sent by this user. • priv - to implement authentication and encryption for SNMP messages sent by this user. This is the highest security level. Note: The settings on the SNMP manager must be set at the same security level or higher than the security level settings on the Switch.

Table 171 Management > Access Control > SNMP > User (continued)

LABEL	DESCRIPTION
Authentication	Select an authentication algorithm. **MD5** (Message Digest 5) and **SHA** (Secure Hash Algorithm) are hash algorithms used to authenticate SNMP data. SHA authentication is generally considered stronger than MD5, but is slower.
Password	Enter the password of up to 32 ASCII characters for SNMP user authentication.
Privacy	Specify the encryption method for SNMP communication from this user. You can choose one of the following: • DES - Data Encryption Standard is a widely used (but breakable) method of data encryption. It applies a 56-bit key to each 64-bit block of data. • AES - Advanced Encryption Standard is another method for data encryption that also uses a secret key. AES applies a 128-bit key to 128-bit blocks of data.
Password	Enter the password of up to 32 ASCII characters for encrypting SNMP packets.
Group	SNMP v3 adopts the concept of View-based Access Control Model (VACM) group. SNMP managers in one group are assigned common access rights to MIBs. Specify in which SNMP group this user is. **admin** - Members of this group can perform all types of system configuration, including the management of administrator accounts. **readwrite** - Members of this group have read and write rights, meaning that the user can create and edit the MIBs on the Switch, except the user account and AAA configuration. **readonly** - Members of this group have read rights only, meaning the user can collect information from the Switch.
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to your previous configuration.
Clear	Click **Clear** to reset the fields to the factory defaults.
Index	This is a read-only number identifying a login account on the Switch. Click on an index number to view more details and edit an existing account.
Username	This field displays the username of a login account on the Switch.
Security Level	This field displays whether you want to implement authentication and/or encryption for SNMP communication with this user.
Authentication	This field displays the authentication algorithm used for SNMP communication with this user.
Privacy	This field displays the encryption method used for SNMP communication with this user.
Group	This field displays the SNMP group to which this user belongs.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to begin configuring this screen afresh.

40.4 Setting Up Login Accounts

Up to five people (one administrator and four non-administrators) may access the Switch via web configurator at any one time.

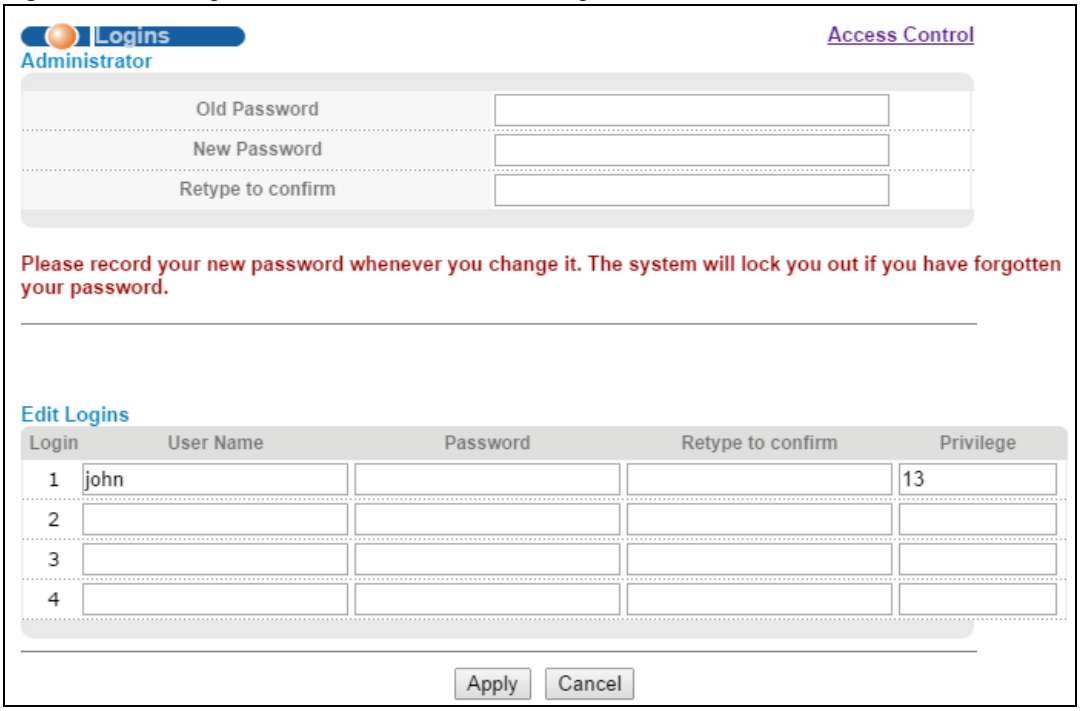
- An administrator is someone who can both view and configure Switch changes. The username for the Administrator is always **admin**. The default administrator password is **1234**.

Note: It is highly recommended that you change the default administrator password (**1234**).

- A non-administrator (username is something other than **admin**) is someone who can view but not configure Switch settings.

Click **Management > Access Control > Logins** to view the screen as shown.

Figure 238 Management > Access Control > Logins



The following table describes the labels in this screen.

Table 172 Management > Access Control > Logins

LABEL	DESCRIPTION
Administrator This is the default administrator account with the “admin” user name. You cannot change the default administrator user name. Only the administrator has read/write access.	
Old Password	Type the existing system password (**1234** is the default password when shipped).
New Password	Enter your new system password.
Retype to confirm	Retype your new system password for confirmation
Edit Logins You may configure passwords for up to four users. These users have read-only access.	
User Name	Set a user name (up to 32 ASCII characters long).
Password	Enter your new system password.
Retype to confirm	Retype your new system password for confirmation

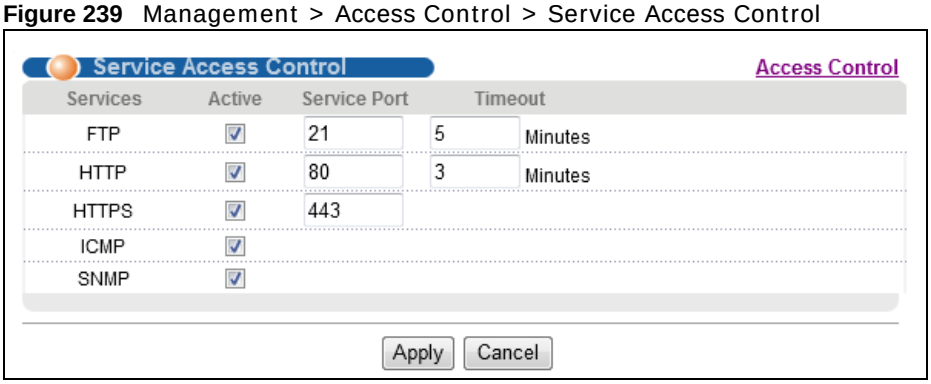
Table 172 Management > Access Control > Logins (continued)

LABEL	DESCRIPTION
Privilege	Type the privilege level for this user. At the time of writing, users may have a privilege level of 0, 3, 13, or 14 representing different configuration rights as shown next. • 0 - Display basic system information. • 3 - Display configuration or status. • 13 - Configure features except for login accounts, SNMP user accounts, the authentication method sequence and authorization settings, multiple logins, administrator and enable passwords, and configuration information display. • 14 - Configure login accounts, SNMP user accounts, the authentication method sequence and authorization settings, multiple logins, and administrator and enable passwords, and display configuration information. Users can run command lines if the session's privilege level is greater than or equal to the command's privilege level. The session privilege initially comes from the privilege of the login account. For example, if the user has a privilege of 5, he/she can run commands that requires privilege level of 5 or less but not more.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

40.5 Service Port Access Control

Service Access Control allows you to decide what services you may use to access the Switch. You may also change the default service port and configure "trusted computer(s)" for each service in the **Remote Management** screen (discussed later). Click **Access Control** to go back to the main **Access Control** screen.

Figure 239 Management > Access Control > Service Access Control



The following table describes the fields in this screen.

Table 173 Management > Access Control > Service Access Control

LABEL	DESCRIPTION
Services	Services you may use to access the Switch are listed here.
Active	Select this option for the corresponding services that you want to allow to access the Switch.
Service Port	For FTP, HTTP or HTTPS services, you may change the default service port by typing the new port number in the **Service Port** field. If you change the default port number then you will have to let people (who wish to use the service) know the new port number for that service.

Table 173 Management > Access Control > Service Access Control (continued)

LABEL	DESCRIPTION
Timeout	Type how many minutes (from 1 to 255) a management session can be left idle before the session times out. After it times out you have to log in with your password again. Very long idle timeouts may have security risks.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

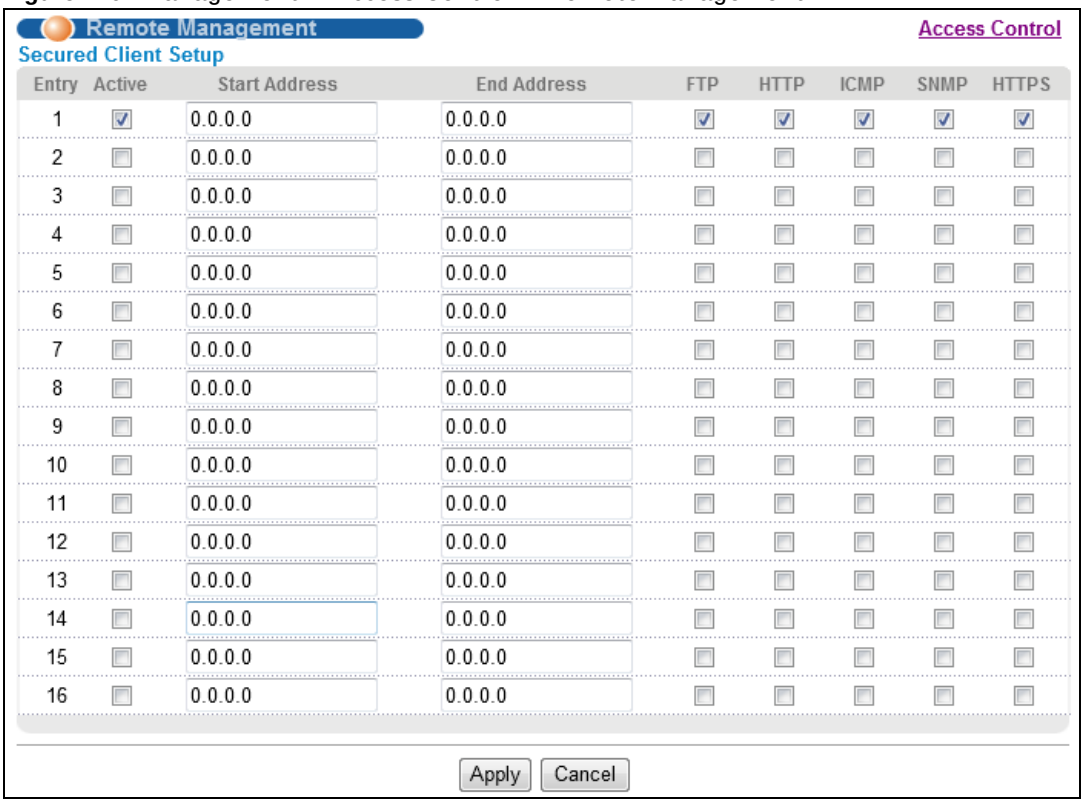
40.6 Remote Management

Use this screen to specify a group of one or more "trusted computers" from which an administrator may use a service to manage the Switch.

Click **Management** > **Access Control** > **Remote Management** to view the screen as shown next.

You can specify a group of one or more "trusted computers" from which an administrator may use a service to manage the Switch. Click **Access Control** to return to the **Access Control** screen.

Figure 240 Management > Access Control > Remote Management



The following table describes the labels in this screen.

Table 174 Management > Access Control > Remote Management

LABEL	DESCRIPTION
Entry	This is the client set index number. A “client set” is a group of one or more “trusted computers” from which an administrator may use a service to manage the Switch.
Active	Select this check box to activate this secured client set. Clear the check box if you wish to temporarily disable the set without deleting it.
Start Address End Address	Configure the IP address range of trusted computers from which you can manage this Switch. The Switch checks if the client IP address of a computer requesting a service or protocol matches the range set here. The Switch immediately disconnects the session if it does not match.
/FTP/HTTP/ ICMP/SNMP/ HTTPS	Select services that may be used for managing the Switch from the specified trusted computers.
Apply	Click **Apply** to save your changes to the Switch’s run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

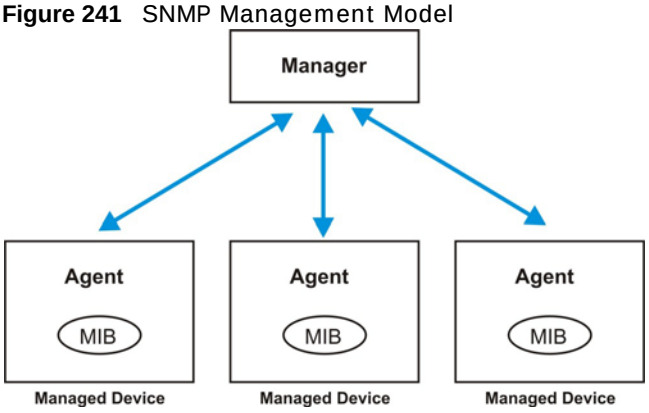
40.7 Technical Reference

This section provides technical background information on the topics discussed in this chapter.

40.7.1 About SNMP

Simple Network Management Protocol (SNMP) is an application layer protocol used to manage and monitor TCP/IP-based devices. SNMP is used to exchange management information between the network management system (NMS) and a network element (NE). A manager station can manage and monitor the Switch through the network via SNMP version 1 (SNMPv1), SNMP version 2c or SNMP version 3. The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

Figure 241 SNMP Management Model



An SNMP managed network consists of two main components: agents and a manager.

An agent is a management software module that resides in a managed Switch (the Switch). An agent translates the local management information from the managed Switch into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a Switch. Examples of variables include number of packets received, node port status and so on. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

Table 175 SNMP Commands

LABEL	DESCRIPTION
Get	Allows the manager to retrieve an object variable from the agent.
GetNext	Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
Set	Allows the manager to set values for object variables within an agent.
Trap	Used by the agent to inform the manager of some events.

SNMP v3 and Security

SNMP v3 enhances security for SNMP management. SNMP managers can be required to authenticate with agents before conducting SNMP management sessions.

Security can be further enhanced by encrypting the SNMP messages sent from the managers. Encryption protects the contents of the SNMP messages. When the contents of the SNMP messages are encrypted, only the intended recipients can read them.

Supported MIBs

MIBs let administrators collect statistics and monitor status and performance.

The Switch supports the following MIBs:

- SNMP MIB II (RFC 1213)
- RFC 1157 SNMP v1
- RFC 1493 Bridge MIBs
- RFC 1643 Ethernet MIBs
- RFC 1155 SMI
- RFC 2674 SNMPv2, SNMPv2c
- RFC 1757 RMON
- SNMPv2, SNMPv2c or later version, compliant with RFC 2011 SNMPv2 MIB for IP, RFC 2012 SNMPv2 MIB for TCP, RFC 2013 SNMPv2 MIB for UDP

SNMP Traps

The Switch sends traps to an SNMP manager when an event occurs. The following tables outline the SNMP traps by category.

Table 176 SNMP System Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
coldstart	coldStart	1.3.6.1.6.3.1.1.5.1	This trap is sent when the Switch is turned on.
warmstart	warmStart	1.3.6.1.6.3.1.1.5.2	This trap is sent when the Switch restarts.
linkup	linkUp	1.3.6.1.6.3.1.1.5.4	This trap is sent when the Ethernet link is up.
linkdown	linkDown	1.3.6.1.6.3.1.1.5.3	This trap is sent when the Ethernet link is down.
lldp	lldpRemTablesChange	1.0.8802.1.1.2.0.0.1	The trap is sent when entries in the remote database have any updates. Link Layer Discovery Protocol (LLDP), defined as IEEE 802.1ab, enables LAN devices that support LLDP to exchange their configured settings. This helps eliminate configuration mismatch issues.
authentication	authenticationFailure	1.3.6.1.6.3.1.1.5.5	This trap is sent when authentication fails due to incorrect user name and/or password.
ping	pingProbeFailed	1.3.6.1.2.1.80.0.1	This trap is sent when a single ping probe fails.
	pingTestFailed	1.3.6.1.2.1.80.0.2	This trap is sent when a ping test (consisting of a series of ping probes) fails.
	pingTestCompleted	1.3.6.1.2.1.80.0.3	This trap is sent when a ping test is completed.
traceroute	traceRouteTestFailed	1.3.6.1.2.1.81.0.2	This trap is sent when a traceroute test fails.
	traceRouteTestCompleted	1.3.6.1.2.1.81.0.3	This trap is sent when a traceroute test is completed.
stp	STPNewRoot	1.3.6.1.2.1.17.0.1	This trap is sent when the STP root switch changes.
	zyMrstpNewRoot	1.3.6.1.4.1.890.1.15.3.52.3.1	This trap is sent when the MRSTP root switch changes.
	zyMstpNewRoot	1.3.6.1.4.1.890.1.15.3.53.3.1	This trap is sent when the MSTP root switch changes.
	STPTopologyChange	1.3.6.1.2.1.17.0.2	This trap is sent when the STP topology changes.
	zyMrstpTopologyChange	1.3.6.1.4.1.890.1.15.3.52.3.2	This trap is sent when the MRSTP topology changes.
	zyMstpTopologyChange	1.3.6.1.4.1.890.1.15.3.53.3.2	This trap is sent when the MSTP root switch changes.

Table 176 SNMP System Traps (continued)

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
rmon	RmonRisingAlarm	1.3.6.1.2.1.16.0.1	This trap is sent when a variable goes over the RMON "rising" threshold.
	RmonFallingAlarm	1.3.6.1.2.1.16.0.2	This trap is sent when the variable falls below the RMON "falling" threshold.

40.7.2 Introduction to HTTPS

HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol that encrypts and decrypts web pages. Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data by ensuring confidentiality (an unauthorized party cannot read the transferred data), authentication (one party can identify the other party) and data integrity (you know if data has been changed).

It relies upon certificates, public keys, and private keys.

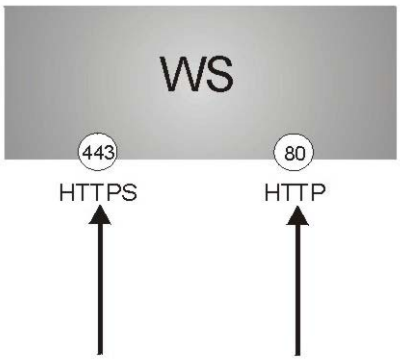
HTTPS on the Switch is used so that you may securely access the Switch using the web configurator. The SSL protocol specifies that the SSL server (the Switch) must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the Switch), whereas the SSL client only should authenticate itself when the SSL server requires it to do so. Authenticating client certificates is optional and if selected means the SSL-client must send the Switch a certificate. You must apply for a certificate for the browser from a Certificate Authority (CA) that is a trusted CA on the Switch.

Please refer to the following figure.

1 HTTPS connection requests from an SSL-aware web browser go to port 443 (by default) on the Switch's WS (web server).

2 HTTP connection requests from a web browser go to port 80 (by default) on the Switch's WS (web server).

Figure 242 HTTPS Implementation



Note: If you disable HTTP in the Service Access Control screen, then the Switch blocks all HTTP connection attempts.

40.7.2.1 HTTPS Example

If you haven't changed the default HTTPS port on the Switch, then in your browser enter "https://Switch IP Address/" as the web site address where "Switch IP Address" is the IP address or domain name of the Switch you wish to access.

Internet Explorer Warning Messages

Internet Explorer 6

When you attempt to access the Switch HTTPS server, a Windows dialog box pops up asking if you trust the server certificate.

You see the following **Security Alert** screen in Internet Explorer. Select **Yes** to proceed to the web configurator login screen; if you select **No**, then web configurator access is blocked.

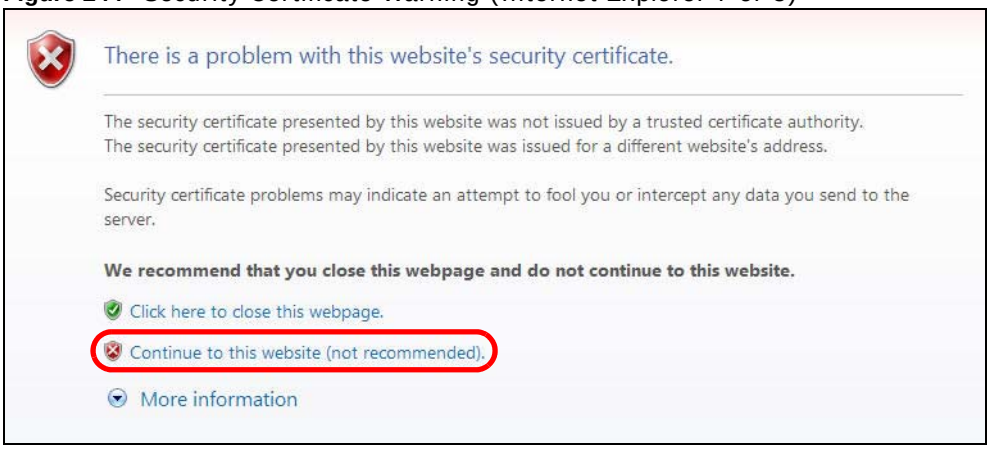
Figure 243 Security Alert Dialog Box (Internet Explorer 6)

Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The name on the security certificate is invalid or does not match the name of the site
Do you want to proceed?
Yes
No
View Certificate

Internet Explorer 7 or 8

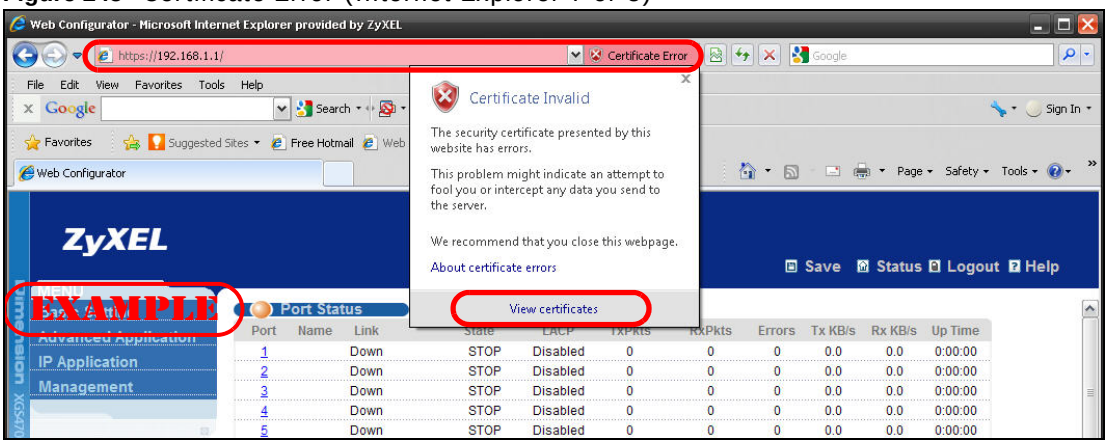
When you attempt to access the Switch HTTPS server, a screen with the message "There is a problem with this website's security certificate." may display. If that is the case, click **Continue to this website (not recommended)** to proceed to the web configurator login screen.

Figure 244 Security Certificate Warning (Internet Explorer 7 or 8)


There is a problem with this website's security certificate.
The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.
Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.
We recommend that you close this webpage and do not continue to this website.
Click here to close this webpage.
Continue to this website (not recommended).
More information

After you log in, you will see the red address bar with the message **Certificate Error**. Click on **Certificate Error** next to the address bar and click **View certificates**.

Figure 245 Certificate Error (Internet Explorer 7 or 8)



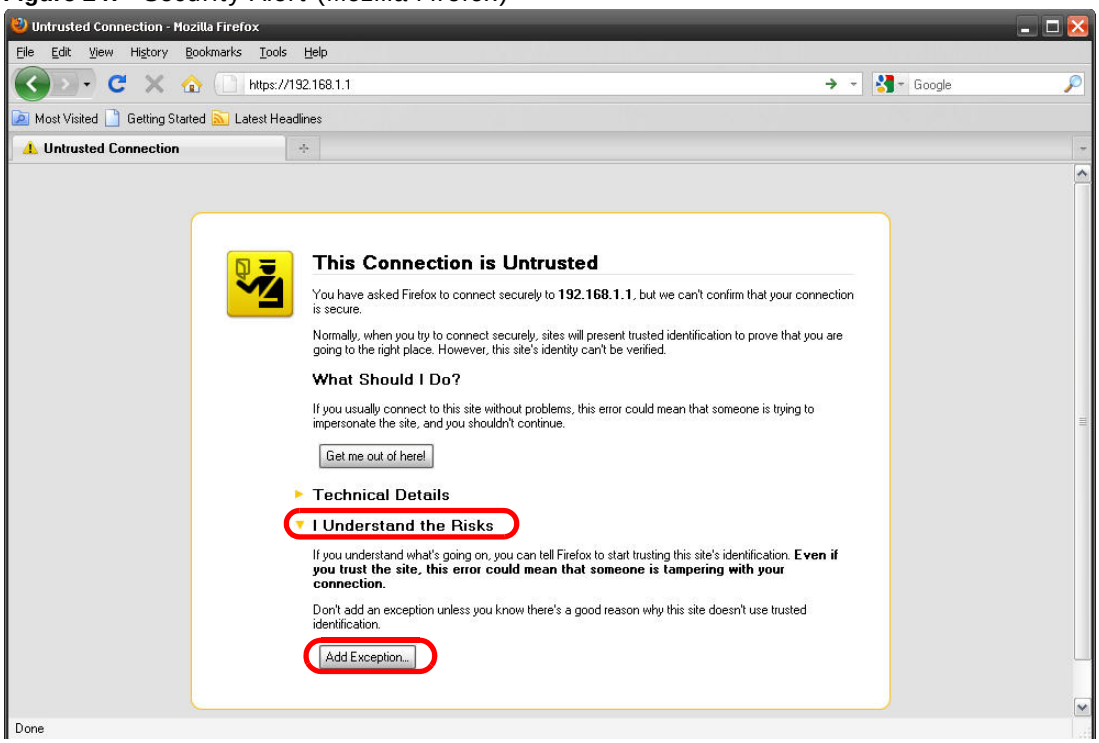
Click **Install Certificate...** and follow the on-screen instructions to install the certificate in your browser.

Figure 246 Certificate (Internet Explorer 7 or 8)

Mozilla Firefox Warning Messages

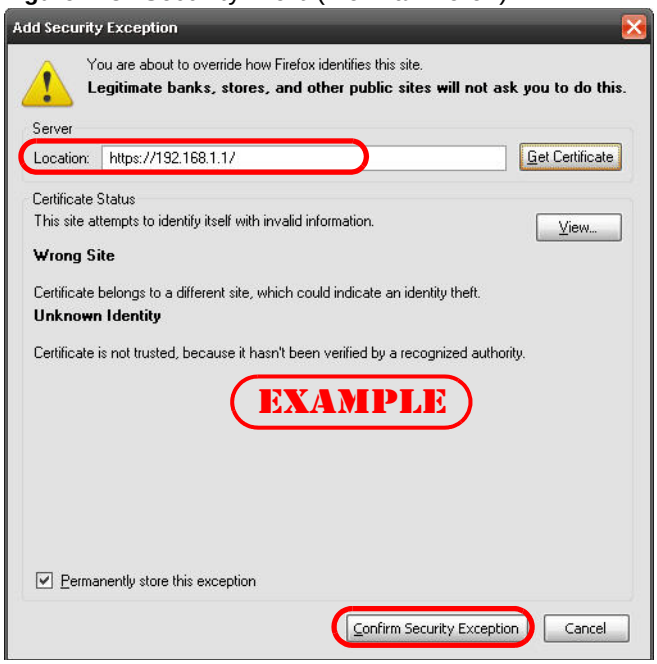
When you attempt to access the Switch HTTPS server, a **This Connection is Unstructed** screen may display. If that is the case, click **I Understand the Risks** and then the **Add Exception...** button.

Figure 247 Security Alert (Mozilla Firefox)


Untrusted Connection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://192.168.1.1
Google
Most Visited Getting Started Latest Headlines
Untrusted Connection
This Connection is Untrusted
You have asked Firefox to connect securely to 192.168.1.1, but we can't confirm that your connection is secure.
Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.
What Should I Do?
If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.
Get me out of here!
Technical Details
I Understand the Risks
If you understand what's going on, you can tell Firefox to start trusting this site's identification. Even if you trust the site, this error could mean that someone is tampering with your connection.
Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.
Add Exception...
Done

Confirm the HTTPS server URL matches. Click **Confirm Security Exception** to proceed to the web configurator login screen.

Figure 248 Security Alert (Mozilla Firefox)

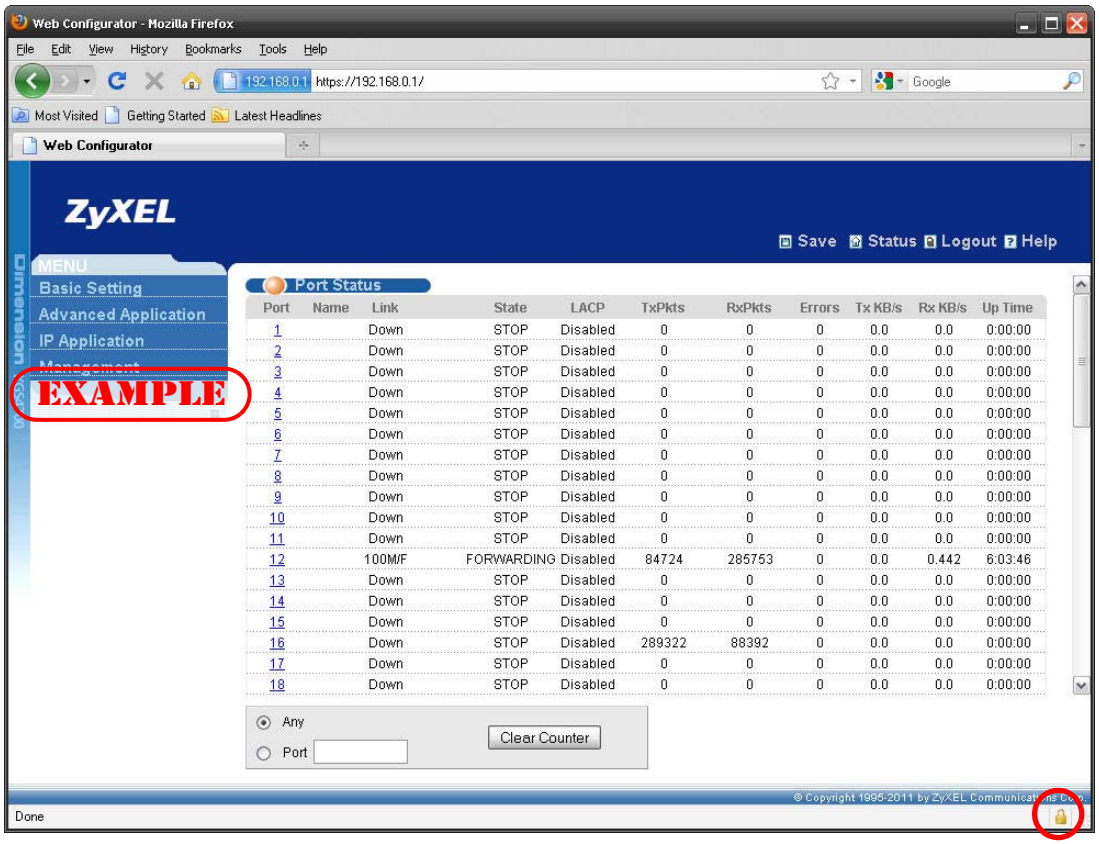

Add Security Exception
You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.
Server
Location: https://192.168.1.1/
Get Certificate
Certificate Status
This site attempts to identify itself with invalid information.
View...
Wrong Site
Certificate belongs to a different site, which could indicate an identity theft.
Unknown Identity
Certificate is not trusted, because it hasn't been verified by a recognized authority.
EXAMPLE
Permanently store this exception
Confirm Security Exception
Cancel

40.7.2.2 The Main Screen

After you accept the certificate and enter the login username and password, the Switch main screen appears. The lock displayed in the bottom right of the browser status bar (in Internet Explorer 6 or

Mozilla Firefox) or next to the address bar (in Internet Explorer 7 or 8) denotes a secure connection.

Figure 249 Example: Lock Denoting a Secure Connection



41 Diagnostic

41.1 Overview

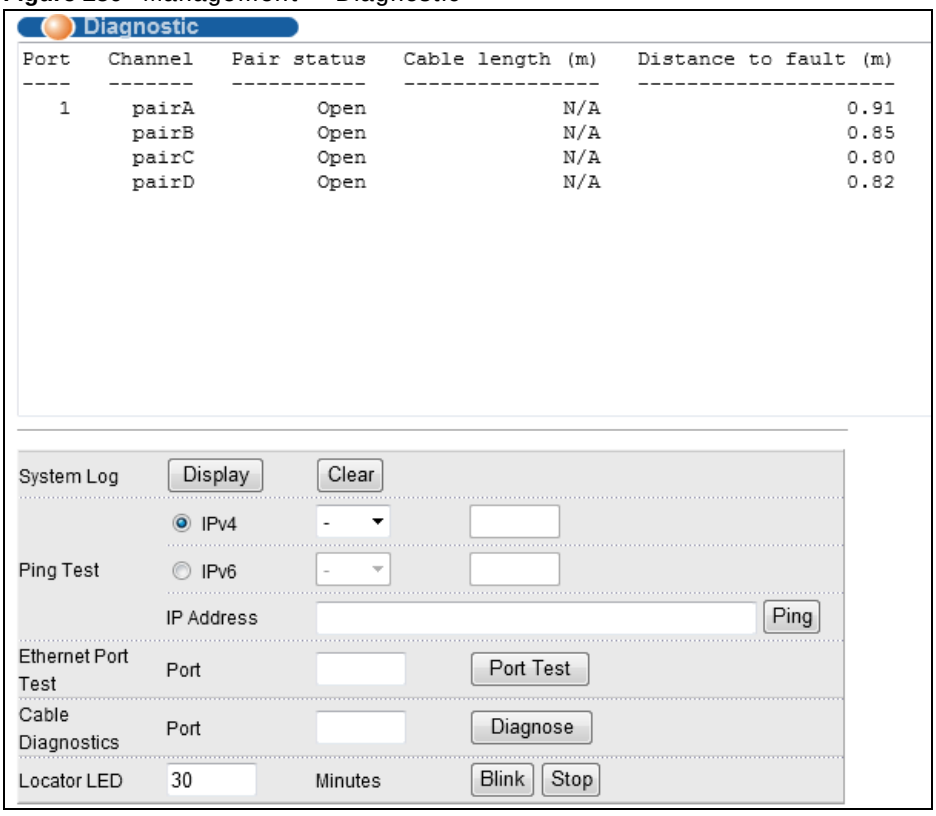
This chapter explains the **Diagnostic** screen.

Use the **Diagnostic** screen (Section 41.2 on page 344) to check system logs, ping IP addresses or perform port tests.

41.2 Diagnostic

Click **Management** > **Diagnostic** in the navigation panel to open this screen. Use this screen to check system logs, ping IP addresses or perform port tests.

Figure 250 Management > Diagnostic



The following table describes the labels in this screen.

Table 177 Management > Diagnostic

LABEL	DESCRIPTION
System Log	Click **Display** to display a log of events in the multi-line text box. Click **Clear** to empty the text box and reset the syslog entry.
Ping Test	
IPv4	Select this option if you want to ping an IPv4 address, and select which traffic flow (**in-band** or **out-of-band**) the Switch is to send ping frames. If you select **in-band**, the Switch sends the frames to all ports except the management port (labelled **MGMT**). If you select **out-of-band**, the Switch sends the frames to the management port (labelled **MGMT**).
IPv6	Select this option if you want to ping an IPv6 address. You also need to select the IPv6 interface type and specify the ID number of interface through which the Switch is to send ping frames.
IP Address	Type the IP address of a device that you want to ping in order to test a connection. Click **Ping** to have the Switch ping the IP address (in the field to the left).
Ethernet Port Test	Enter a port number and click **Port Test** to perform an internal loopback test.
Cable Diagnostics	Enter a port number and click **Diagnose** to perform a physical wire-pair test of the Ethernet connections on the specified port(s). The following fields display when you diagnose a port.
Port	This is the number of the physical Ethernet port on the Switch.
Channel	An Ethernet cable usually has four pairs of wires. A 10BASE-T or 100BASE-TX port only use and test two pairs, while a 1000BASE-T port requires all four pairs. This displays the descriptive name of the wire-pair in the cable.
Pair status	**Ok**: The physical connection between the wire-pair is okay. **Open**: There is no physical connection (an open circuit detected) between the wire-pair. **Short**: There is an short circuit detected between the wire-pair. **Unknown**: The Switch failed to run cable diagnostics on the cable connected this port. **Unsupported**: The port is a fiber port or it is not active.
Cable length	This displays the total length of the Ethernet cable that is connected to the port when the **Pair status** is **Ok** and the Switch chipset supports this feature. This shows **N/A** if the **Pair status** is **Open** or **Short**. Check the **Distance to fault**. This shows **Unsupported** if the Switch chipset does not support to show the cable length.
Distance to fault	This displays the distance between the port and the location where the cable is open or shorted. This shows **N/A** if the **Pair status** is **Ok**. This shows **Unsupported** if the Switch chipset does not support to show the distance.
Locator LED	Enter a time interval (in minutes) and click **Blink** to show the actual location of the Switch between several devices in a rack. The default time interval is 30 minutes. Click **Stop** to have the Switch terminate the blinking locator LED.

42

Syslog

42.1 Syslog Overview

This chapter explains the syslog screens.

The syslog protocol allows devices to send event notification messages across an IP network to syslog servers that collect the event messages. A syslog-enabled device can generate a syslog message and send it to a syslog server.

Syslog is defined in RFC 3164. The RFC defines the packet format, content and system log related information of syslog messages. Each syslog message has a facility and severity level. The syslog facility identifies a file in the syslog server. Refer to the documentation of your syslog program for details. The following table describes the syslog severity levels.

Table 178 Syslog Severity Levels

CODE	SEVERITY
0	Emergency: The system is unusable.
1	Alert: Action must be taken immediately.
2	Critical: The system condition is critical.
3	Error: There is an error condition on the system.
4	Warning: There is a warning condition on the system.
5	Notice: There is a normal but significant condition on the system.
6	Informational: The syslog contains an informational message.
7	Debug: The message is intended for debug-level purposes.

42.1.1 What You Can Do

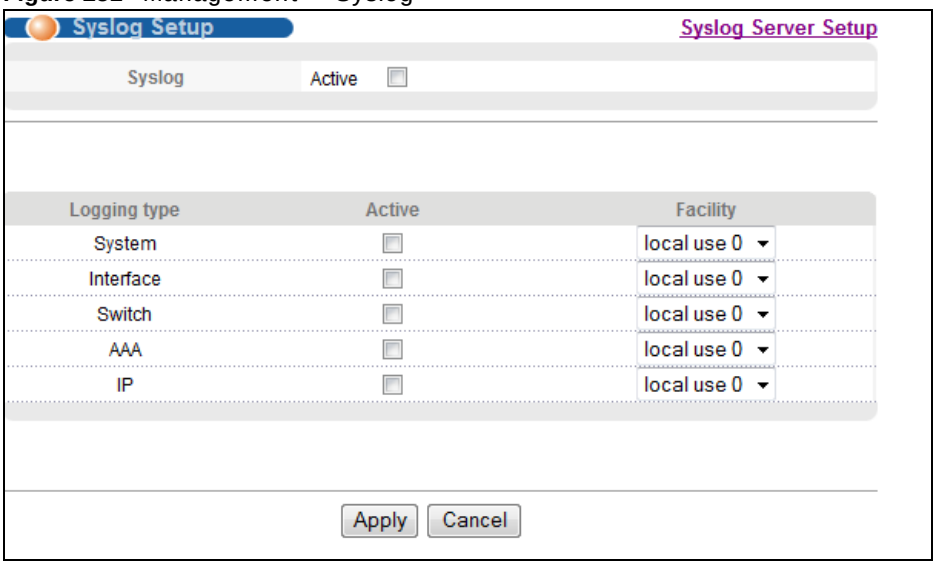
- Use the **Syslog Setup** screen (Section 42.2 on page 346) to configure the device's system logging settings.
- Use the **Syslog Server Setup** screen (Section 42.3 on page 347) to configure a list of external syslog servers.

42.2 Syslog Setup

Use this screen to configure the device's system logging settings.

Click **Management** > **Syslog** in the navigation panel to display this screen. The syslog feature sends logs to an external syslog server.

Figure 251 Management > Syslog



The following table describes the labels in this screen.

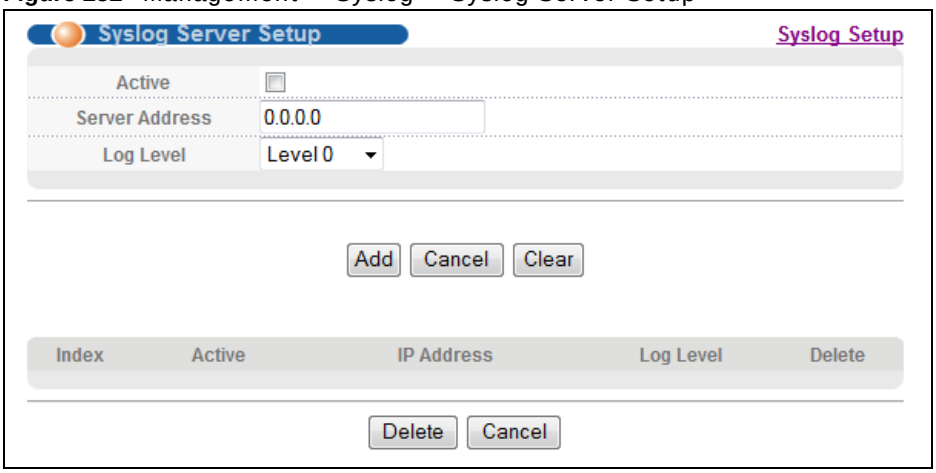
Table 179 Management > Syslog

LABEL	DESCRIPTION
Syslog	Select **Active** to turn on syslog (system logging) and then configure the syslog setting
Logging Type	This column displays the names of the categories of logs that the device can generate.
Active	Select this option to set the device to generate logs for the corresponding category.
Facility	The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

42.3 Syslog Server Setup

Click **Management** > **Syslog** > **Syslog Server Setup** to view the screen as shown next. Use this screen to configure a list of external syslog servers.

Figure 252 Management > Syslog > Syslog Server Setup



The following table describes the labels in this screen.

Table 180 Management > Syslog > Syslog Server Setup

LABEL	DESCRIPTION
Active	Select this check box to have the device send logs to this syslog server. Clear the check box if you want to create a syslog server entry but not have the device send logs to it (you can edit the entry later).
Server Address	Enter the IP address of the syslog server.
Log Level	Select the severity level(s) of the logs that you want the device to send to this syslog server. The lower the number, the more critical the logs are.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to return the fields to the factory defaults.
Index	This is the index number of a syslog server entry. Click this number to edit the entry.
Active	This field displays **Yes** if the device is to send logs to the syslog server. **No** displays if the device is not to send logs to the syslog server.
IP Address	This field displays the IP address of the syslog server.
Log Level	This field displays the severity level of the logs that the device is to send to this syslog server.
Delete	Select an entry's **Delete** check box and click **Delete** to remove the entry.
Cancel	Click **Cancel** to begin configuring this screen afresh.

43

Cluster Management

43.1 Cluster Management Overview

This chapter introduces cluster management.

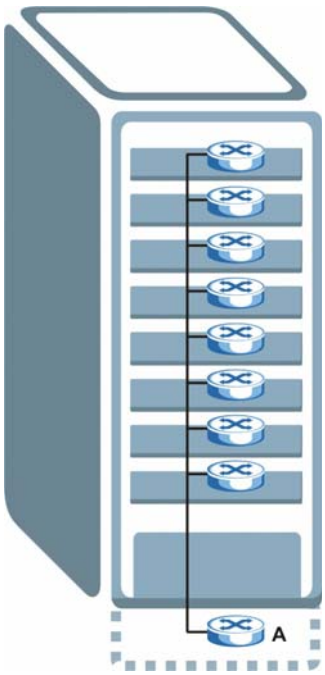
Cluster Management allows you to manage switches through one Switch, called the cluster manager. The switches must be directly connected and be in the same VLAN group so as to be able to communicate with one another.

Table 181 ZyXEL Clustering Management Specifications

Maximum number of cluster members	24
Cluster Member Models	Must be compatible with ZyXEL cluster management implementation.
Cluster Manager	The switch through which you manage the cluster member switches.
Cluster Members	The switches being managed by the cluster manager switch.

In the following example, switch **A** in the basement is the cluster manager and the other switches on the upper floors of the building are cluster members.

Figure 253 Clustering Application Example



43.1.1 What You Can Do

- Use the **Cluster Management** screen (Section 43.2 on page 350) to view the role of the Switch within the cluster and to access a cluster member switch's web configurator.
- Use the **Clustering Management Configuration** screen (Section 43.1 on page 349) to configure clustering management.

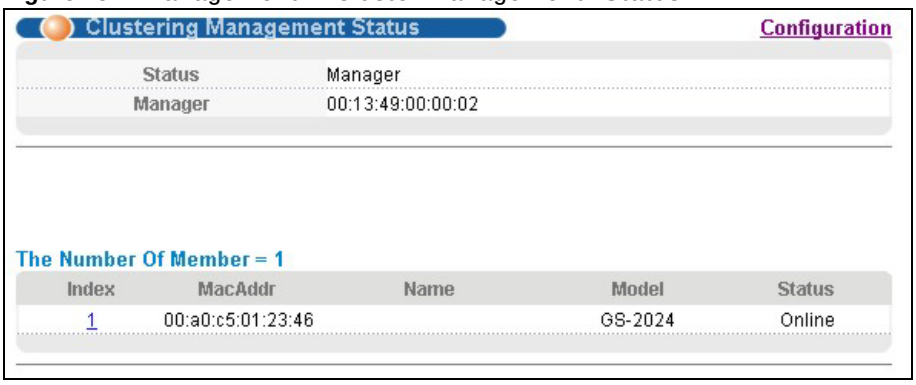
43.2 Cluster Management Status

Use this screen to view the role of the Switch within the cluster and to access a cluster member switch's web configurator.

Click **Management** > **Cluster Management** in the navigation panel to display the following screen.

Note: A cluster can only have one manager.

Figure 254 Management > Cluster Management: Status



The following table describes the labels in this screen.

Table 182 Management > Cluster Management: Status

LABEL	DESCRIPTION
Status	This field displays the role of this Switch within the cluster. **Manager** **Member** (you see this if you access this screen in the cluster member switch directly and not via the cluster manager) **None** (neither a manager nor a member of a cluster)
Manager	This field displays the cluster manager switch's hardware MAC address.
The Number of Member	This field displays the number of switches that make up this cluster. The following fields describe the cluster member switches.
Index	You can manage cluster member switches via the cluster manager switch. Each number in the **Index** column is a hyperlink leading to the cluster member switch's web configurator (see Figure 256 on page 353).
MacAddr	This is the cluster member switch's hardware MAC address.
Name	This is the cluster member switch's **System Name**.

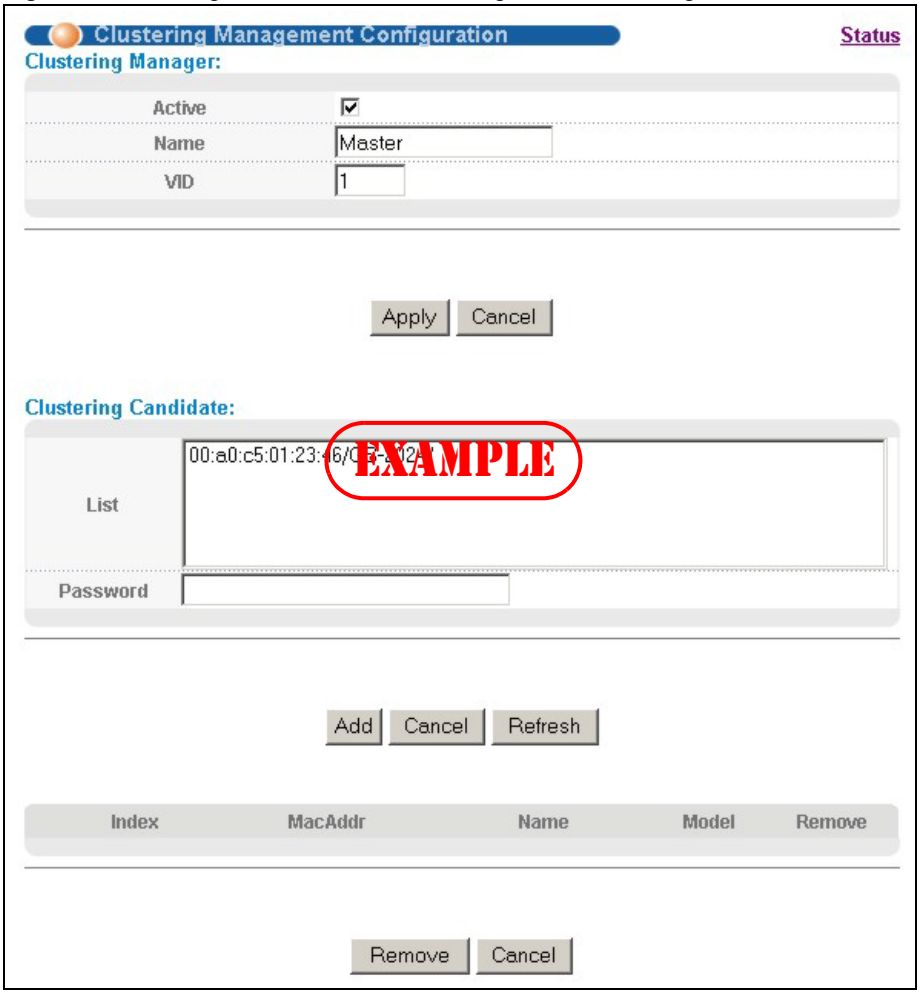
Table 182 Management > Cluster Management: Status (continued)

LABEL	DESCRIPTION
Model	This field displays the model name.
Status	This field displays: **Online** (the cluster member switch is accessible) **Error** (for example the cluster member switch password was changed or the switch was set as the manager and so left the member list, etc.) **Offline** (the switch is disconnected - **Offline** shows approximately 1.5 minutes after the link between cluster member and manager goes down)

43.3 Clustering Management Configuration

Use this screen to configure clustering management. Click **Management** > **Cluster Management** > **Configuration** to display the next screen.

Figure 255 Management > Cluster Management > Configuration



The following table describes the labels in this screen.

Table 183 Management > Cluster Management > Configuration

LABEL	DESCRIPTION
Clustering Manager	
Active	Select **Active** to have this Switch become the cluster manager switch. A cluster can only have one manager. Other (directly connected) switches that are set to be cluster managers will not be visible in the **Clustering Candidates** list. If a switch that was previously a cluster member is later set to become a cluster manager, then its **Status** is displayed as **Error** in the **Cluster Management Status** screen and a warning icon (⚠) appears in the member summary list below.
Name	Type a name to identify the **Clustering Manager.** You may use up to 32 printable characters (spaces are allowed).
VID	This is the VLAN ID and is only applicable if the Switch is set to **802.1Q** VLAN. All switches must be directly connected and in the same VLAN group to belong to the same cluster. Switches that are not in the same VLAN group are not visible in the **Clustering Candidates** list. This field is ignored if the **Clustering Manager** is using **Port-based** VLAN.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clustering Candidate	The following fields relate to the switches that are potential cluster members.
List	A list of suitable candidates found by auto-discovery is shown here. The switches must be directly connected. Directly connected switches that are set to be cluster managers will not be visible in the **Clustering Candidate** list. Switches that are not in the same management VLAN group will not be visible in the **Clustering Candidate** list.
Password	Each cluster member's password is its web configurator password. Select a member in the **Clustering Candidate** list and then enter its web configurator password. If that switch administrator changes the web configurator password afterwards, then it cannot be managed from the **Cluster Manager**. Its **Status** is displayed as **Error** in the **Cluster Management Status** screen and a warning icon (⚠) appears in the member summary list below. If multiple devices have the same password then hold [SHIFT] and click those switches to select them. Then enter their common web configurator password.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Refresh	Click **Refresh** to perform auto-discovery again to list potential cluster members.
The next summary table shows the information for the clustering members configured.	
Index	This is the index number of a cluster member switch.
MacAddr	This is the cluster member switch's hardware MAC address.
Name	This is the cluster member switch's **System Name**.
Model	This is the cluster member switch's model name.
Remove	Select this checkbox and then click the **Remove** button to remove a cluster member switch from the cluster.
Cancel	Click **Cancel** to begin configuring this screen afresh.

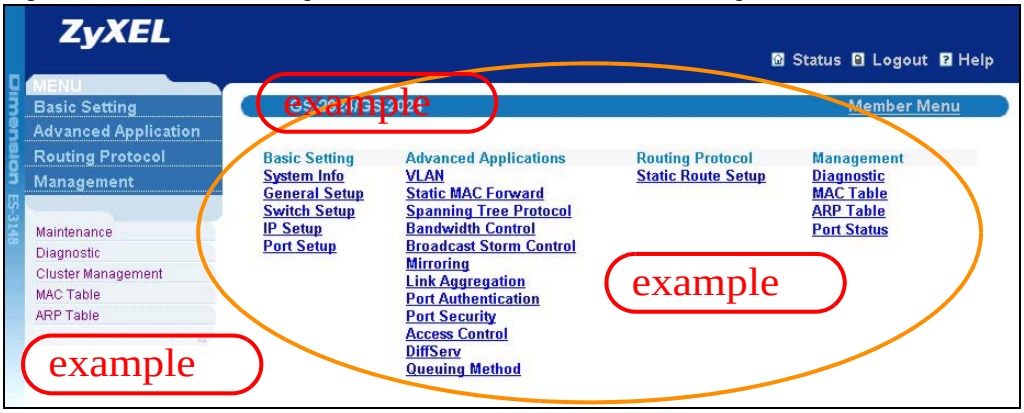
43.4 Technical Reference

This section provides technical background information on the topics discussed in this chapter.

43.4.1 Cluster Member Switch Management

Go to the **Clustering Management Status** screen of the cluster manager switch and then select an **Index** hyperlink from the list of members to go to that cluster member switch's web configurator home page. This cluster member web configurator home page and the home page that you'd see if you accessed it directly are different.

Figure 256 Cluster Management: Cluster Member Web Configurator Screen



43.4.1.1 Uploading Firmware to a Cluster Member Switch

You can use FTP to upload firmware to a cluster member switch through the cluster manager switch as shown in the following example.

Figure 257 Example: Uploading Firmware to a Cluster Member Switch

```
C:\>ftp 192.168.1.1
Connected to 192.168.1.1.
220 Switch FTP version 1.0 ready at Thu Jan  1 00:58:46 1970
User (192.168.0.1:(none)): admin
331 Enter PASS command
Password:
230 Logged in
ftp> ls
200 Port command okay
150 Opening data connection for LIST
--w--w--w-   1 owner    group         3042210 Jul 01 12:00 ras
-rw-rw-rw-   1 owner    group          393216 Jul 01 12:00 config
--w--w--w-   1 owner    group               0 Jul 01 12:00 fw-00-a0-c5-01-23-46
-rw-rw-rw-   1 owner    group               0 Jul 01 12:00 config-00-a0-c5-01-23-46
226 File sent OK
ftp: 297 bytes received in 0.00Seconds 297000.00Kbytes/sec.
ftp> bin
200 Type I OK
ftp> put 410AAHW0.bin fw-00-a0-c5-01-23-46
200 Port command okay
150 Opening data connection for STOR fw-00-a0-c5-01-23-46
226 File received OK
ftp: 262144 bytes sent in 0.63Seconds 415.44Kbytes/sec.
ftp>
```

The following table explains some of the FTP parameters.

Table 184 FTP Upload to Cluster Member Example

FTP PARAMETER	DESCRIPTION
User	Enter “admin”.
Password	The web configurator password default is 1234.
ls	Enter this command to list the name of cluster member switch’s firmware and configuration file.
410AAHW0.bin	This is the name of the firmware file you want to upload to the cluster member switch.
fw-00-a0-c5-01-23-46	This is the cluster member switch’s firmware name as seen in the cluster manager switch.
config-00-a0-c5-01-23-46	This is the cluster member switch’s configuration file name as seen in the cluster manager switch.

44

MAC Table

44.1 MAC Table Overview

This chapter introduces the **MAC Table** screen.

The **MAC Table** screen (a MAC table is also known as a filtering database) shows how frames are forwarded or filtered across the Switch's ports. It shows what device MAC address, belonging to what VLAN group (if any) is forwarded to which port(s) and whether the MAC address is dynamic (learned by the Switch) or static (manually entered in the **Static MAC Forwarding** screen).

44.1.1 What You Can Do

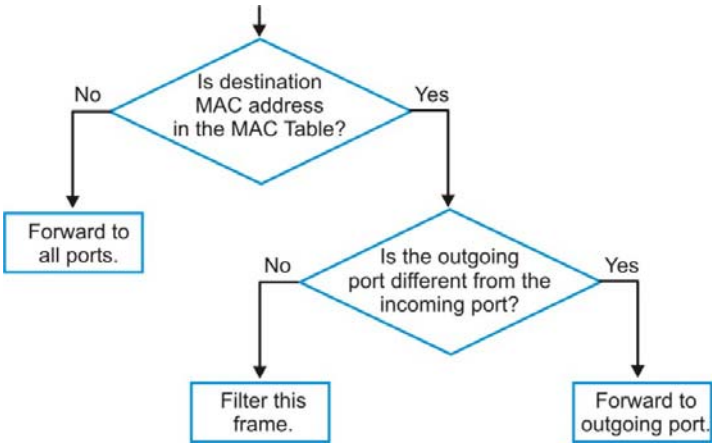
Use the **MAC Table** screen (Section 44.2 on page 356) to check whether the MAC address is dynamic or static.

44.1.2 What You Need to Know

The Switch uses the MAC table to determine how to forward frames. See the following figure.

1. The Switch examines a received frame and learns the port on which this source MAC address came.
2. The Switch checks to see if the frame's destination MAC address matches a source MAC address already learned in the MAC table.
   - If the Switch has already learned the port for this MAC address, then it forwards the frame to that port.
   - If the Switch has not already learned the port for this MAC address, then the Switch sends an ARP to request the MAC address. The Switch then learns the port that replies with the MAC address.
   - If the Switch has already learned the port for this MAC address, but the destination port is the same as the port it came in on, then it filters the frame.

Figure 258 MAC Table Flowchart

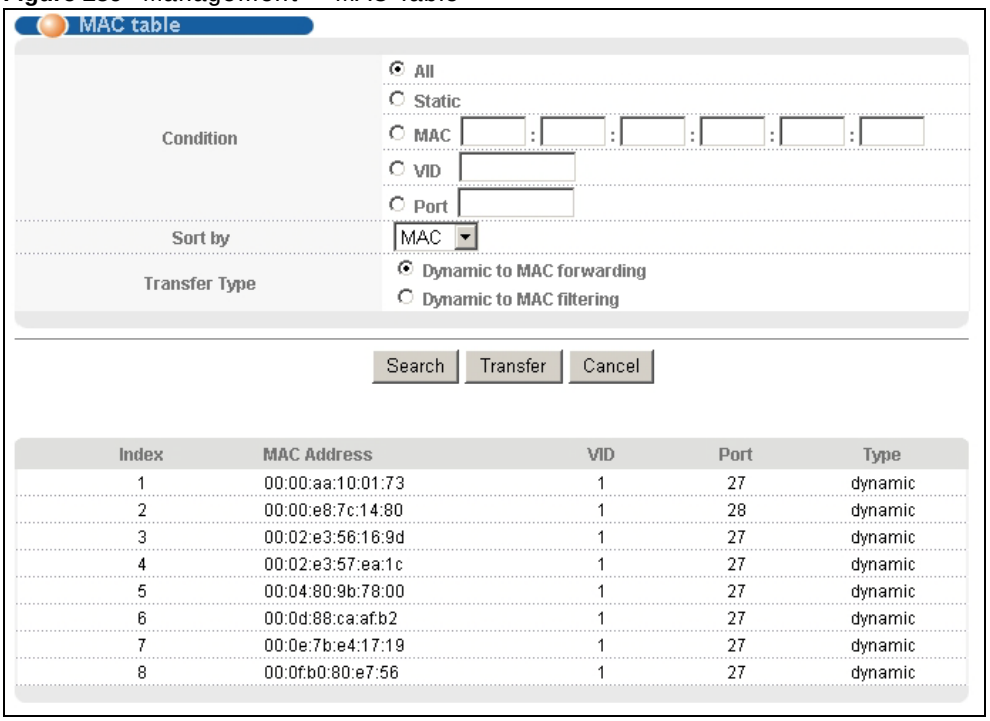


44.2 Viewing the MAC Table

Use this screen to check whether the MAC address is dynamic or static.

Click **Management** > **MAC Table** in the navigation panel to display the following screen.

Figure 259 Management > MAC Table



The following table describes the labels in this screen.

Table 185 Management > MAC Table

LABEL	DESCRIPTION
Condition	Select one of the buttons and click **Search** to only display the data which matches the criteria you specified. Select **All** to display any entry in the MAC table of the Switch. Select **Static** to display the MAC entries manually configured on the Switch. Select **MAC** and enter a MAC address in the field provided to display a specified MAC entry. Select **VID** and enter a VLAN ID in the field provided to display the MAC entries belonging to the specified VLAN. Select **Port** and enter a port number in the field provided to display the MAC addresses which are forwarded on the specified port.
Sort by	Define how the Switch displays and arranges the data in the summary table below. Select **MAC** to display and arrange the data according to MAC address. Select **VID** to display and arrange the data according to VLAN group. Select **PORT** to display and arrange the data according to port number.
Transfer Type	Select **Dynamic to MAC forwarding** and click the **Transfer** button to change all dynamically learned MAC address entries in the summary table below into static entries. They also display in the **Static MAC Forwarding** screen. Select **Dynamic to MAC filtering** and click the **Transfer** button to change all dynamically learned MAC address entries in the summary table below into MAC filtering entries. These entries will then display only in the **Filtering** screen and the default filtering action is **Discard source**.
Cancel	Click **Cancel** to change the fields back to their last saved values.
Index	This is the incoming frame index number.
MAC Address	This is the MAC address of the device from which this incoming frame came.
VID	This is the VLAN group to which this frame belongs.
Port	This is the port where the above MAC address is forwarded.
Type	This shows whether the MAC address is **dynamic** (learned by the Switch) or **static** (manually entered in the **Static MAC Forwarding** screen).

45

IP Table

This chapter introduces the IP table.

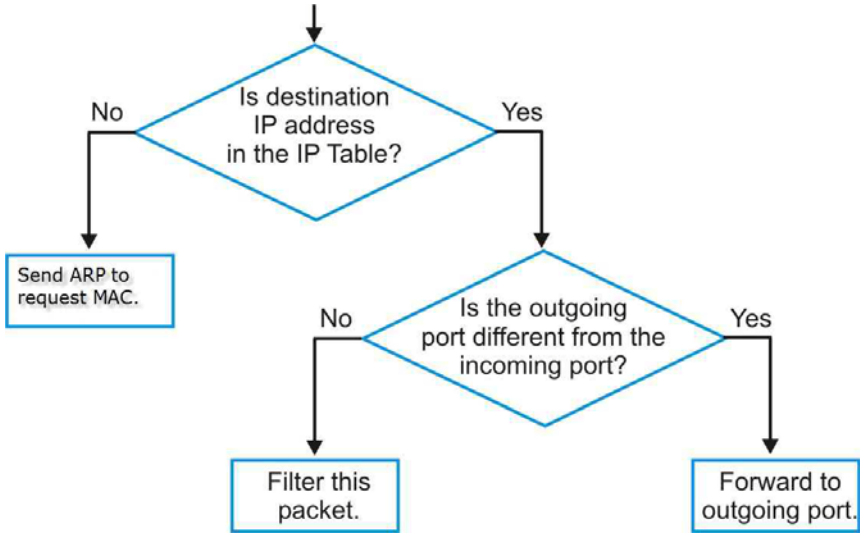
45.1 IP Table Overview

The **IP Table** screen shows how packets are forwarded or filtered across the Switch's ports. When a device (which may belong to a VLAN group) sends a packet which is forwarded to a port on the Switch, the IP address of the device is shown on the Switch's **IP Table**. The **IP Table** also shows whether the IP address is dynamic (learned by the Switch) or static (belonging to the Switch).

The Switch uses the **IP Table** to determine how to forward packets. See the following figure.

1. The Switch examines a received packet and learns the port from which this source IP address came.
2. The Switch checks to see if the packet's destination IP address matches a source IP address already learned in the **IP Table**.
   - If the Switch has already learned the port for this IP address, then it forwards the packet to that port.
   - If the Switch has not already learned the port for this IP address, then the Switch sends an ARP to request the MAC address. The Switch then learns the port that replies with the MAC address.
   - If the Switch has already learned the port for this IP address, but the destination port is the same as the port it came in on, then it filters the packet.

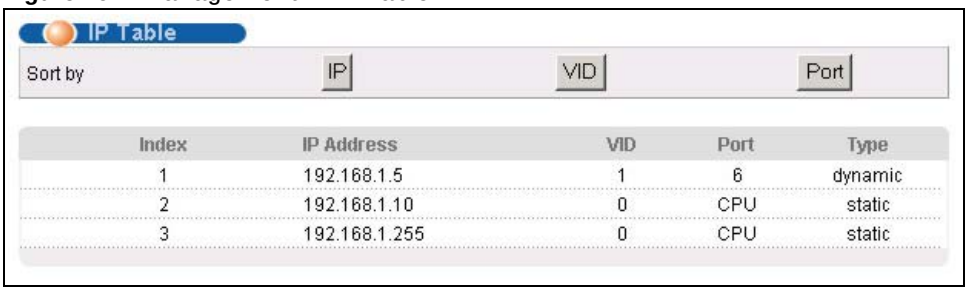
Figure 260 IP Table Flowchart



45.2 Viewing the IP Table

Click **Management** > **IP Table** in the navigation panel to display the following screen.

Figure 261 Management > IP Table



The following table describes the labels in this screen.

Table 186 Management > IP Table

LABEL	DESCRIPTION
Sort by	Click one of the following buttons to display and arrange the data according to that button type. The information is then displayed in the summary table below.
IP	Click this button to display and arrange the data according to IP address.
VID	Click this button to display and arrange the data according to VLAN group.
Port	Click this button to display and arrange the data according to port number.
Index	This field displays the index number.
IP Address	This is the IP address of the device from which the incoming packets came.
VID	This is the VLAN group to which the packet belongs.
Port	This is the port from which the above IP address was learned. This field displays **CPU** to indicate the IP address belongs to the Switch.
Type	This shows whether the IP address is **dynamic** (learned by the Switch) or **static** (belonging to the Switch).

46

ARP Table

46.1 Overview

This chapter introduces ARP Table.

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control or MAC address, on the local area network.

An IP (version 4) address is 32 bits long. In an Ethernet LAN, MAC addresses are 48 bits long. The ARP Table maintains an association between each MAC address and its corresponding IP address.

46.1.1 What You Can Do

Use the **ARP Table** screen (Section 46.2 on page 360) to view IP-to-MAC address mapping(s).

46.1.2 What You Need to Know

When an incoming packet destined for a host device on a local area network arrives at the Switch, the Switch's ARP program looks in the ARP Table and if it finds the address, it sends it to the device.

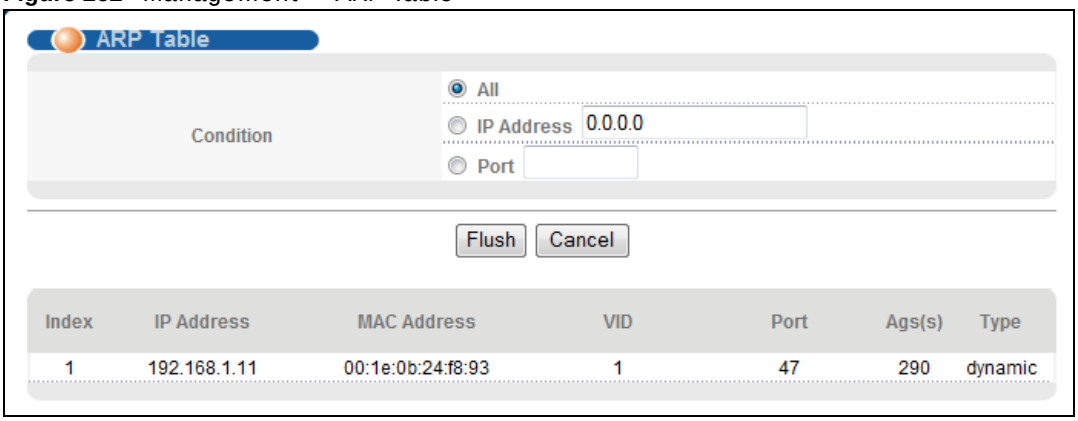
If no entry is found for the IP address, ARP broadcasts the request to all the devices on the LAN. The Switch fills in its own MAC and IP address in the sender address fields, and puts the known IP address of the target in the target IP address field. In addition, the Switch puts all ones in the target MAC field (FF.FF.FF.FF.FF.FF is the Ethernet broadcast address). The replying device (which is either the IP address of the device being sought or the router that knows the way) replaces the broadcast address with the target's MAC address, swaps the sender and target pairs, and unicasts the answer directly back to the requesting machine. ARP updates the ARP Table for future reference and then sends the packet to the MAC address that replied.

46.2 Viewing the ARP Table

Use the ARP table to view IP-to-MAC address mapping(s) and remove specific dynamic ARP entries.

Click **Management > ARP Table** in the navigation panel to open the following screen.

Figure 262 Management > ARP Table



The following table describes the labels in this screen.

Table 187 Management > ARP Table

LABEL	DESCRIPTION
Condition	Specify how you want the Switch to remove ARP entries when you click **Flush**. Select **All** to remove all of the dynamic entries from the ARP table. Select **IP Address** and enter an IP address to remove the dynamic entries learned with the specified IP address. Select **Port** and enter a port number to remove the dynamic entries learned on the specified port.
Flush	Click **Flush** to remove the ARP entries according to the condition you specified.
Cancel	Click **Cancel** to return the fields to the factory defaults.
Index	This is the ARP table entry number.
IP Address	This is the IP address of a device connected to a Switch port with the corresponding MAC address below.
MAC Address	This is the MAC address of the device with the corresponding IP address above.
VID	This field displays the VLAN to which the device belongs.
Port	This field displays the port to which the device connects. **CPU** means this IP address is the Switch's management IP address.
Age(s)	This field displays how long (in seconds) an entry can still remain in the ARP table before it ages out and needs to be relearned. This shows **0** for a static entry.
Type	This shows whether the IP address is dynamic (learned by the Switch) or static (manually configured in the **Basic Setting > IP Setup** or **IP Application > ARP Setup > Static ARP** screen).

47

Routing Table

This chapter introduces the routing table.

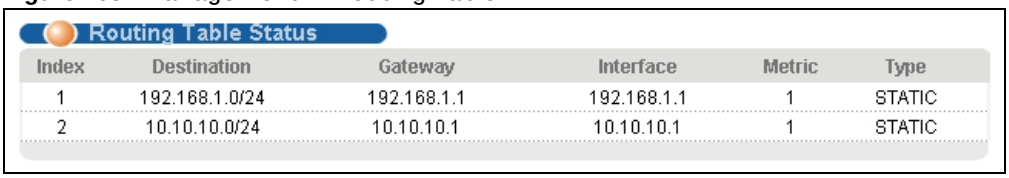
47.1 Overview

The routing table contains the route information to the network(s) that the Switch can reach.

47.2 Viewing the Routing Table Status

Use this screen to view routing table information. Click **Management** > **Routing Table** in the navigation panel to display the screen as shown.

Figure 263 Management > Routing Table



The following table describes the labels in this screen.

Table 188 Management > Routing Table

LABEL	DESCRIPTION
Index	This field displays the index number.
Destination	This field displays the destination IP routing domain.
Gateway	This field displays the IP address of the gateway device.
Interface	This field displays the IP address of the Interface.
Metric	This field displays the cost of the route.
Type	This field displays the method used to learn the route. **STATIC** - added as a static entry.

48

Path MTU Table

This chapter introduces the IPv6 Path MTU table.

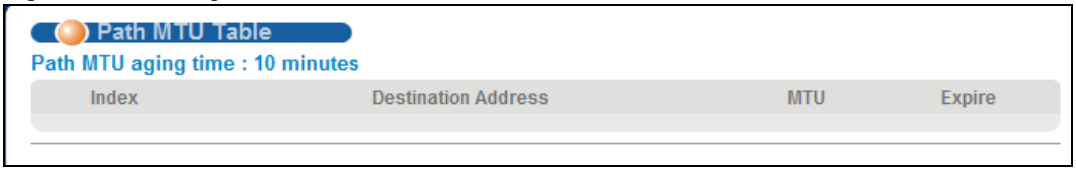
48.1 Path MTU Overview

The largest size (in bytes) of a packet that can be transferred over a data link is called the maximum transmission unit (MTU). The Switch uses Path MTU Discovery to discover Path MTU (PMTU), that is, the minimum link MTU of all the links in a path to the destination. If the Switch receives an ICMPv6 Packet Too Big error message after sending a packet, it fragments the next packet according to the suggested MTU in the error message.

48.2 Viewing the Path MTU Table

Use this screen to view IPv6 path MTU information on the Switch. Click **Management** > **Path MTU Table** in the navigation panel to display the screen as shown.

Figure 264 Management > Path MTU Table



The following table describes the labels in this screen.

Table 189 Management > Path MTU Table

LABEL	DESCRIPTION
Path MTU aging time	This field displays how long an entry remains in the Path MTU table before it ages out and needs to be relearned.
Index	This field displays the index number of each entry in the table.
Destination Address	This field displays the destination IPv6 address of each path/entry.
MTU	This field displays the maximum transmission unit of the links in the path.
Expire	This field displays how long (in minutes) an entry can still remain in the Path MTU table before it ages out and needs to be relearned.

49

Configure Clone

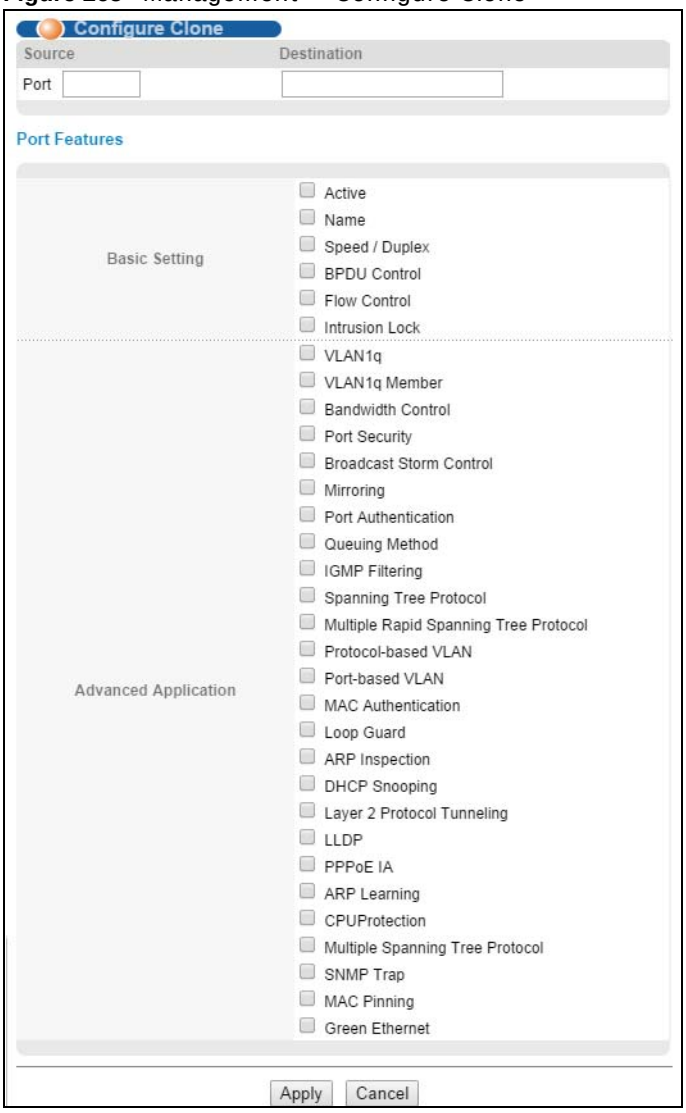
49.1 Overview

This chapter shows you how you can copy the settings of one port onto other ports.

49.2 Configure Clone

Cloning allows you to copy the basic and advanced settings from a source port to a destination port or ports. Click **Management** > **Configure Clone** to open the following screen.

Figure 265 Management > Configure Clone



The following table describes the labels in this screen.

Table 190 Management > Configure Clone

LABEL	DESCRIPTION
Source/ Destination Port	Enter the source port under the **Source** label. This port's attributes are copied. Enter the destination port or ports under the **Destination** label. These are the ports which are going to have the same attributes as the source port. You can enter individual ports separated by a comma or a range of ports by using a dash. Example: **2, 4, 6** indicates that ports 2, 4 and 6 are the destination ports. **2-6** indicates that ports 2 through 6 are the destination ports.
Basic Setting	Select which port settings (you configured in the **Basic Setting** menus) should be copied to the destination port(s).
Advanced Application	Select which port settings (you configured in the **Advanced Application** menus) should be copied to the destination ports.

Table 190 Management > Configure Clone (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

50

Neighbor Table

This chapter introduces the IPv6 neighbor table.

50.1 IPv6 Neighbor Table Overview

An IPv6 host is required to have a neighbor table. If there is an address to be resolved or verified, the Switch sends out a neighbor solicitation message. When the Switch receives a neighbor advertisement in response, it stores the neighbor's link-layer address in the neighbor table. You can also manually create a static IPv6 neighbor entry using the **Basic Setting > IPv6 > IPv6 Configuration > IPv6 Neighbor Setup** screen.

When the Switch needs to send a packet, it first consults other table to determine the next hop. Once the next hop IPv6 address is known, the Switch looks into the neighbor table to get the link-layer address and sends the packet when the neighbor is reachable. If the Switch cannot find an entry in the neighbor table or the state for the neighbor is not reachable, it starts the address resolution process. This helps reduce the number of IPv6 solicitation and advertisement messages.

50.2 Viewing the IPv6 Neighbor Table

Use this screen to view IPv6 neighbor information on the Switch. Click **Management** > **Neighbor Table** in the navigation panel to display the screen as shown.

Figure 266 Management > Neighbor Table

The following table describes the labels in this screen.

Table 191 Management > Neighbor Table

LABEL	DESCRIPTION
Index	This field displays the index number of each entry in the table.
Interface	This field displays the ID number of the IPv6 interface on which the IPv6 address is created or through which the neighboring device can be reached.
Neighbor Address	This field displays the IPv6 address of the Switch or a neighboring device.
MAC	This field displays the MAC address of the IPv6 interface on which the IPv6 address is configure or the MAC address of the neighboring device.

Table 191 Management > Neighbor Table (continued)

LABEL	DESCRIPTION
Status	This field displays whether the neighbor IPv6 interface is reachable. In IPv6, “reachable” means an IPv6 packet can be correctly forwarded to a neighbor node (host or router) and the neighbor can successfully receive and handle the packet. The available options in this field are: • reachable (R): The interface of the neighboring device is reachable. (The Switch has received a response to the initial request.) • stale (S): The last reachable time has expired and the Switch is waiting for a response to another initial request. The field displays this also when the Switch receives an unrequested response from the neighbor’s interface. • delay (D): The neighboring interface is no longer known to be reachable, and traffic has been sent to the neighbor recently. The Switch delays sending request packets for a short to give upper-layer protocols a chance to determine reachability. • probe (P): The Switch is sending request packets and waiting for the neighbor’s response. • invalid (IV): The neighbor address is with an invalid IPv6 address. • unknown (?): The status of the neighboring interface can not be determined for some reason. • incomplete (I): Address resolution is in progress and the link-layer address of the neighbor has not yet been determined. The interface of the neighboring device did not give a complete response.
Type	This field displays the type of an address mapping to a neighbor interface. The available options in this field are: • other (O): none of the following type. • local (L): A Switch interface is using the address. • dynamic (D): The IP address to MAC address can be successfully resolved using IPv6 Neighbor Discovery protocol. Is it similar as IPv4 ARP (Address Resolution protocol). • static (S): The interface address is statically configured.

51

Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- Switch Access and Login
- Switch Configuration

51.1 Power, Hardware Connections, and LEDs

The Switch does not turn on. None of the LEDs turn on.

1. Make sure you are using the power adaptor or cord included with the Switch.
2. Make sure the power adaptor or cord is connected to the Switch and plugged in to an appropriate power source. Make sure the power source is turned on.
3. Disconnect and re-connect the power adaptor or cord to the Switch.
4. If the problem continues, contact the vendor.

The **ALM** LED is on.

1. Disconnect and re-connect the power adaptor or cord to the Switch.
2. If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See Section 3.3 on page 29.
2. Check the hardware connections. See Section 51.1 on page 369.
3. Inspect your cables for damage. Contact the vendor to replace any damaged cables.

4 Disconnect and re-connect the power adaptor or cord to the Switch.

5 If the problem continues, contact the vendor.

51.2 Switch Access and Login

I forgot the IP address for the Switch.

1 The default IP address is **192.168.1.1**.

2 If this does not work, you have to reset the device to its factory defaults. See Section 3.4 on page 29.

I forgot the username and/or password.

1 The default username is **admin** and the default password is **1234**.

2 If this does not work, you have to reset the device to its factory defaults. See Section 3.4 on page 29.

I cannot see or access the **Login** screen in the web configurator.

1 Make sure you are using the correct IP address.

- The default IP address is 192.168.1.1.
- If you changed the IP address, use the new IP address.
- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I forgot the IP address for the Switch.

2 Check the hardware connections, and make sure the LEDs are behaving as expected. See Section 3.3 on page 29.

3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled.

4 Make sure your computer is in the same subnet as the Switch. (If you know that there are routers between your computer and the Switch, skip this step.)

5 Reset the device to its factory defaults, and try to access the Switch with the default IP address. See Section 3.4 on page 29. If the problem continues, contact the vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Try to access the Switch using another service, such as FTP. If you can access the Switch, check the remote management settings to find out why the Switch does not respond to HTTP.

I can see the **Login** screen, but I cannot log in to the Switch.

1. Make sure you have entered the user name and password correctly. The default user name is **admin**, and the default password is **1234**. These fields are case-sensitive, so make sure [Caps Lock] is not on.
2. You may have exceeded the maximum number of concurrent sessions.

   Check that you have enabled logins for HTTP. If you have configured a secured client IP address, your computer's IP address must match it. Refer to the chapter on access control for details.
3. Disconnect and re-connect the cord to the Switch.
4. If this does not work, you have to reset the device to its factory defaults. See Section 3.4 on page 29.

Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

I cannot see some of **Advanced Application** submenus at the bottom of the navigation panel.

The recommended screen resolution is 1024 by 768 pixels. Adjust the value in your computer and then you should see the rest of **Advanced Application** submenus at the bottom of the navigation panel.

There is unauthorized access to my Switch.

Click the **Display** button in the **System Log** field in the **Management** > **Diagnostic** screen to check for unauthorized access to your Switch. To avoid unauthorized access, configure the secured client setting in the **Management** > **Access Control** > **Remote Management** screen. Computers not belonging to the secured client set cannot get permission to access the Switch.

51.3 Switch Configuration

I lost my configuration settings after I restart the Switch.

Make sure you save your configuration into the Switch's nonvolatile memory each time you make changes. Click **Save** at the top right corner of the web configurator to save the configuration permanently. See also Section 39.2.3 on page 321 for more information about how to save your configuration.

A

Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device. Regional websites are listed below.

See also *http://www.zyxel.com/about_zyxel/zyxel_worldwide.shtml*.

Please have the following information ready when you contact an office.

Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Corporate Headquarters (Worldwide)

Taiwan

- ZyXEL Communications Corporation
- http://www.zyxel.com

Asia

China

- ZyXEL Communications (Shanghai) Corp.
  ZyXEL Communications (Beijing) Corp.
  ZyXEL Communications (Tianjin) Corp.
- http://www.zyxel.cn

India

- ZyXEL Technology India Pvt Ltd
- http://www.zyxel.in

Kazakhstan

- ZyXEL Kazakhstan
- http://www.zyxel.kz

Korea

- ZyXEL Korea Corp.
- http://www.zyxel.kr

Malaysia

- ZyXEL Malaysia Sdn Bhd.
- http://www.zyxel.com.my

Pakistan

- ZyXEL Pakistan (Pvt.) Ltd.
- http://www.zyxel.com.pk

Philipines

- ZyXEL Philippines
- http://www.zyxel.com.ph

Singapore

- ZyXEL Singapore Pte Ltd.
- http://www.zyxel.com.sg

Taiwan

- ZyXEL Communications Corporation
- http://www.zyxel.com

Thailand

- ZyXEL Thailand Co., Ltd
- http://www.zyxel.co.th

Vietnam

- ZyXEL Communications Corporation-Vietnam Office
- http://www.zyxel.com/vn/vi

Europe

Austria

- ZyXEL Deutschland GmbH
- http://www.zyxel.de

Belarus

- ZyXEL BY
- http://www.zyxel.by

Belgium

- ZyXEL Communications B.V.
- http://www.zyxel.com/be/nl/

Bulgaria

- ZyXEL България
- http://www.zyxel.com/bg/bg/

Czech

- ZyXEL Communications Czech s.r.o
- http://www.zyxel.cz

Denmark

- ZyXEL Communications A/S
- http://www.zyxel.dk

Estonia

- ZyXEL Estonia
- http://www.zyxel.com/ee/et/

Finland

- ZyXEL Communications
- http://www.zyxel.fi

France

- ZyXEL France
- http://www.zyxel.fr

Germany

- ZyXEL Deutschland GmbH
- http://www.zyxel.de

Hungary

- ZyXEL Hungary & SEE
- http://www.zyxel.hu

Latvia

- ZyXEL Latvia

- http://www.zyxel.com/lv/lv/homepage.shtml

Lithuania

- ZyXEL Lithuania
- http://www.zyxel.com/lt/lt/homepage.shtml

Netherlands

- ZyXEL Benelux
- http://www.zyxel.nl

Norway

- ZyXEL Communications
- http://www.zyxel.no

Poland

- ZyXEL Communications Poland
- http://www.zyxel.pl

Romania

- ZyXEL Romania
- http://www.zyxel.com/ro/ro

Russia

- ZyXEL Russia
- http://www.zyxel.ru

Slovakia

- ZyXEL Communications Czech s.r.o. organizacna zlozka
- http://www.zyxel.sk

Spain

- ZyXEL Spain
- http://www.zyxel.es

Sweden

- ZyXEL Communications
- http://www.zyxel.se

Switzerland

- Studerus AG

- http://www.zyxel.ch/

Turkey

- ZyXEL Turkey A.S.
- http://www.zyxel.com.tr

UK

- ZyXEL Communications UK Ltd.
- http://www.zyxel.co.uk

Ukraine

- ZyXEL Ukraine
- http://www.ua.zyxel.com

Latin America

Argentina

- ZyXEL Communication Corporation
- http://www.zyxel.com/ec/es/

Ecuador

- ZyXEL Communication Corporation
- http://www.zyxel.com/ec/es/

Middle East

Egypt

- ZyXEL Communication Corporation
- http://www.zyxel.com/homepage.shtml

Middle East

- ZyXEL Communication Corporation
- http://www.zyxel.com/homepage.shtml

North America

USA

- ZyXEL Communications, Inc. - North America Headquarters
- http://www.us.zyxel.com/

Oceania

Australia

- ZyXEL Communications Corporation
- http://www.zyxel.com/au/en/

Africa

South Africa

- Nology (Pty) Ltd.
- http://www.zyxel.co.za

B

Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **User-Defined**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 192 Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example www.zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.

Table 192 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	Simple File Transfer Protocol.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).

Table 192 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another videoconferencing solution.

C

IPv6

Overview

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4 x 10^{38} IP addresses.

IPv6 Addressing

The 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address `2001:0db8:1a2b:0015:0000:0000:1a2f:0000`.

IPv6 addresses can be abbreviated in two ways:

- Leading zeros in a block can be omitted. So `2001:0db8:1a2b:0015:0000:0000:1a2f:0000` can be written as `2001:db8:1a2b:15:0:0:1a2f:0`.
- Any number of consecutive blocks of zeros can be replaced by a double colon. A double colon can only appear once in an IPv6 address. So `2001:0db8:0000:0000:1a2f:0000:0000:0015` can be written as `2001:0db8::1a2f:0000:0000:0015`, `2001:0db8:0000:0000:1a2f::0015`, `2001:db8::1a2f:0:0:15` or `2001:db8:0:0:1a2f::15`.

Prefix and Prefix Length

Similar to an IPv4 subnet mask, IPv6 uses an address prefix to represent the network address. An IPv6 prefix length specifies how many most significant bits (start from the left) in the address compose the network address. The prefix length is written as “/x” where x is a number. For example,

```
2001:db8:1a2b:15::1a2f:0/32
```

means that the first 32 bits (`2001:db8`) is the subnet prefix.

Link-local Address

A link-local address uniquely identifies a device on the local network (the LAN). It is similar to a “private IP address” in IPv4. You can have the same link-local address on multiple interfaces on a device. A link-local unicast address has a predefined prefix of fe80::/10. The link-local unicast address format is as follows.

Table 193 Link-local Unicast Address Format

1111 1110 10	0	Interface ID
10 bits	54 bits	64 bits

Global Address

A global address uniquely identifies a device on the Internet. It is similar to a “public IP address” in IPv4. A global unicast address starts with a 2 or 3.

Unspecified Address

An unspecified address (0:0:0:0:0:0:0:0 or ::) is used as the source address when a device does not have its own address. It is similar to “0.0.0.0” in IPv4.

Loopback Address

A loopback address (0:0:0:0:0:0:0:1 or ::1) allows a host to send packets to itself. It is similar to “127.0.0.1” in IPv4.

Multicast Address

In IPv6, multicast addresses provide the same functionality as IPv4 broadcast addresses. Broadcasting is not supported in IPv6. A multicast address allows a host to send packets to all hosts in a multicast group.

Multicast scope allows you to determine the size of the multicast group. A multicast address has a predefined prefix of ff00::/8. The following table describes some of the predefined multicast addresses.

Table 194 Predefined Multicast Address

MULTICAST ADDRESS	DESCRIPTION
FF01:0:0:0:0:0:0:1	All hosts on a local node.
FF01:0:0:0:0:0:0:2	All routers on a local node.
FF02:0:0:0:0:0:0:1	All hosts on a local connected link.
FF02:0:0:0:0:0:0:2	All routers on a local connected link.
FF05:0:0:0:0:0:0:2	All routers on a local site.
FF05:0:0:0:0:0:1:3	All DHCP severs on a local site.

The following table describes the multicast addresses which are reserved and can not be assigned to a multicast group.

Table 195 Reserved Multicast Address

MULTICAST ADDRESS
FF00:0:0:0:0:0:0:0
FF01:0:0:0:0:0:0:0
FF02:0:0:0:0:0:0:0
FF03:0:0:0:0:0:0:0
FF04:0:0:0:0:0:0:0
FF05:0:0:0:0:0:0:0
FF06:0:0:0:0:0:0:0
FF07:0:0:0:0:0:0:0
FF08:0:0:0:0:0:0:0
FF09:0:0:0:0:0:0:0

Table 195 Reserved Multicast Address (continued)

MULTICAST ADDRESS
FF0A:0:0:0:0:0:0:0
FF0B:0:0:0:0:0:0:0
FF0C:0:0:0:0:0:0:0
FF0D:0:0:0:0:0:0:0
FF0E:0:0:0:0:0:0:0
FF0F:0:0:0:0:0:0:0

Subnet Masking

Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses four bits for each character (1 ~ 10, A ~ F). Each block's 16 bits are then represented by four hexadecimal characters. For example, FFFF:FFFF:FFFF:FFFF:FC00:0000:0000:0000.

Interface ID

In IPv6, an interface ID is a 64-bit identifier. It identifies a physical interface (for example, an Ethernet port) or a virtual interface (for example, the management IP address for a VLAN). One interface should have a unique interface ID.

EUI-64

The EUI-64 (Extended Unique Identifier) defined by the IEEE (Institute of Electrical and Electronics Engineers) is an interface ID format designed to adapt with IPv6. It is derived from the 48-bit (6-byte) Ethernet MAC address as shown next. EUI-64 inserts the hex digits fffe between the third and fourth bytes of the MAC address and complements the seventh bit of the first byte of the MAC address. See the following example.

Table 196

MAC	00	:	13	:	49	:	12	:	34	:	56

Table 197

EUI-64	02	:	13	:	49	:	FF	:	FE	:	12	:	34	:	56

Stateless Autoconfiguration

With stateless autoconfiguration in IPv6, addresses can be uniquely and automatically generated. Unlike DHCPv6 (Dynamic Host Configuration Protocol version six) which is used in IPv6 stateful autoconfiguration, the owner and status of addresses don't need to be maintained by a DHCP server. Every IPv6 device is able to generate its own and unique IP address automatically when IPv6 is initiated on its interface. It combines the prefix and the interface ID (generated from its own Ethernet MAC address, see Interface ID and EUI-64) to form a complete IPv6 address.

When IPv6 is enabled on a device, its interface automatically generates a link-local address (beginning with fe80).

When the interface is connected to a network with a router and the Switch is set to automatically obtain an IPv6 network prefix from the router for the interface, it generates [2]another address which

combines its interface ID and global and subnet information advertised from the router. This is a routable global IP address.

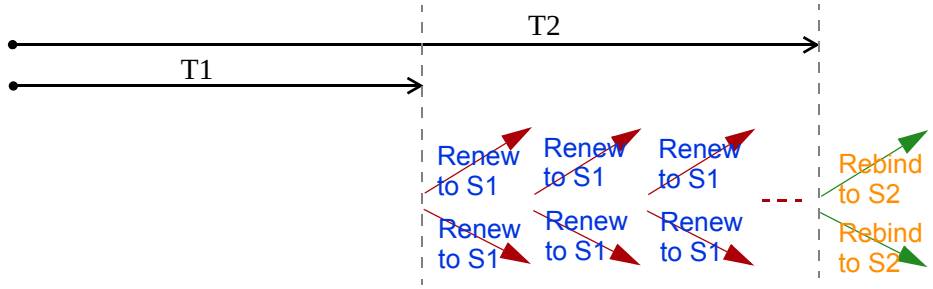
DHCPv6

The Dynamic Host Configuration Protocol for IPv6 (DHCPv6, RFC 3315) is a server-client protocol that allows a DHCP server to assign and pass IPv6 network addresses, prefixes and other configuration information to DHCP clients. DHCPv6 servers and clients exchange DHCP messages using UDP.

Each DHCP client and server has a unique DHCP Unique IDentifier (DUID), which is used for identification when they are exchanging DHCPv6 messages. The DUID is generated from the MAC address, time, vendor assigned ID and/or the vendor's private enterprise number registered with the IANA. It should not change over time even after you reboot the device.

Identity Association

An Identity Association (IA) is a collection of addresses assigned to a DHCP client, through which the server and client can manage a set of related IP addresses. Each IA must be associated with exactly one interface. The DHCP client uses the IA assigned to an interface to obtain configuration from a DHCP server for that interface. Each IA consists of a unique IAID and associated IP information.
The IA type is the type of address in the IA. Each IA holds one type of address. IA_NA means an identity association for non-temporary addresses and IA_TA is an identity association for temporary addresses. An IA_NA option contains the T1 and T2 fields, but an IA_TA option does not. The DHCPv6 server uses T1 and T2 to control the time at which the client contacts with the server to extend the lifetimes on any addresses in the IA_NA before the lifetimes expire. After T1, the client sends the server (**S1**) (from which the addresses in the IA_NA were obtained) a Renew message. If the time T2 is reached and the server does not respond, the client sends a Rebind message to any available server (**S2**). For an IA_TA, the client may send a Renew or Rebind message at the client's discretion.



DHCP Relay Agent

A DHCP relay agent is on the same network as the DHCP clients and helps forward messages between the DHCP server and clients. When a client cannot use its link-local address and a well-known multicast address to locate a DHCP server on its network, it then needs a DHCP relay agent to send a message to a DHCP server that is not attached to the same network.

The DHCP relay agent can add the remote identification (remote-ID) option and the interface-ID option to the Relay-Forward DHCPv6 messages. The remote-ID option carries a user-defined string,

2. In IPv6, all network interfaces can be associated with several addresses.

such as the system name. The interface-ID option provides slot number, port information and the VLAN ID to the DHCPv6 server. The remote-ID option (if any) is stripped from the Relay-Reply messages before the relay agent sends the packets to the clients. The DHCP server copies the interface-ID option from the Relay-Forward message into the Relay-Reply message and sends it to the relay agent. The interface-ID should not change even after the relay agent restarts.

Prefix Delegation

Prefix delegation enables an IPv6 router to use the IPv6 prefix (network address) received from the ISP (or a connected uplink router) for its LAN. The Switch uses the received IPv6 prefix (for example, 2001:db2::/48) to generate its LAN IP address. Through sending Router Advertisements (RAs) regularly by multicast, the Switch passes the IPv6 prefix information to its LAN hosts. The hosts then can use the prefix to generate their IPv6 addresses.

ICMPv6

Internet Control Message Protocol for IPv6 (ICMPv6 or ICMP for IPv6) is defined in RFC 4443. ICMPv6 has a preceding Next Header value of 58, which is different from the value used to identify ICMP for IPv4. ICMPv6 is an integral part of IPv6. IPv6 nodes use ICMPv6 to report errors encountered in packet processing and perform other diagnostic functions, such as "ping".

Neighbor Discovery Protocol (NDP)

The Neighbor Discovery Protocol (NDP) is a protocol used to discover other IPv6 devices and track neighbor's reachability in a network. An IPv6 device uses the following ICMPv6 messages types:

- Neighbor solicitation: A request from a host to determine a neighbor's link-layer address (MAC address) and detect if the neighbor is still reachable. A neighbor being "reachable" means it responds to a neighbor solicitation message (from the host) with a neighbor advertisement message.
- Neighbor advertisement: A response from a node to announce its link-layer address.
- Router solicitation: A request from a host to locate a router that can act as the default router and forward packets.
- Router advertisement: A response to a router solicitation or a periodical multicast advertisement from a router to advertise its presence and other parameters.

IPv6 Cache

An IPv6 host is required to have a neighbor cache, destination cache, prefix list and default router list. The Switch maintains and updates its IPv6 caches constantly using the information from response messages. In IPv6, the Switch configures a link-local address automatically, and then sends a neighbor solicitation message to check if the address is unique. If there is an address to be resolved or verified, the Switch also sends out a neighbor solicitation message. When the Switch receives a neighbor advertisement in response, it stores the neighbor's link-layer address in the neighbor cache. When the Switch uses a router solicitation message to query for a router and receives a router advertisement message, it adds the router's information to the neighbor cache, prefix list and destination cache. The Switch creates an entry in the default router list cache if the router can be used as a default router.

When the Switch needs to send a packet, it first consults the destination cache to determine the next hop. If there is no matching entry in the destination cache, the Switch uses the prefix list to

determine whether the destination address is on-link and can be reached directly without passing through a router. If the address is onlink, the address is considered as the next hop. Otherwise, the Switch determines the next-hop from the default router list or routing table. Once the next hop IP address is known, the Switch looks into the neighbor cache to get the link-layer address and sends the packet when the neighbor is reachable. If the Switch cannot find an entry in the neighbor cache or the state for the neighbor is not reachable, it starts the address resolution process. This helps reduce the number of IPv6 solicitation and advertisement messages.

Example - Enabling IPv6 on Windows XP/2003/Vista

By default, Windows XP and Windows 2003 support IPv6. This example shows you how to use the `ipv6 install` command on Windows XP/2003 to enable IPv6. This also displays how to use the `ipconfig` command to see auto-generated IP addresses.

```
C:\>ipv6 install
Installing...
Succeeded.

C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 10.1.1.46
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        IP Address. . . . . . . . . . . . : fe80::2d0:59ff:feb8:103c%4
        Default Gateway . . . . . . . . . : 10.1.1.254
```

IPv6 is installed and enabled by default in Windows Vista. Use the `ipconfig` command to check your automatic configured IPv6 address as well. You should see at least one IPv6 address available for the interface on your computer.

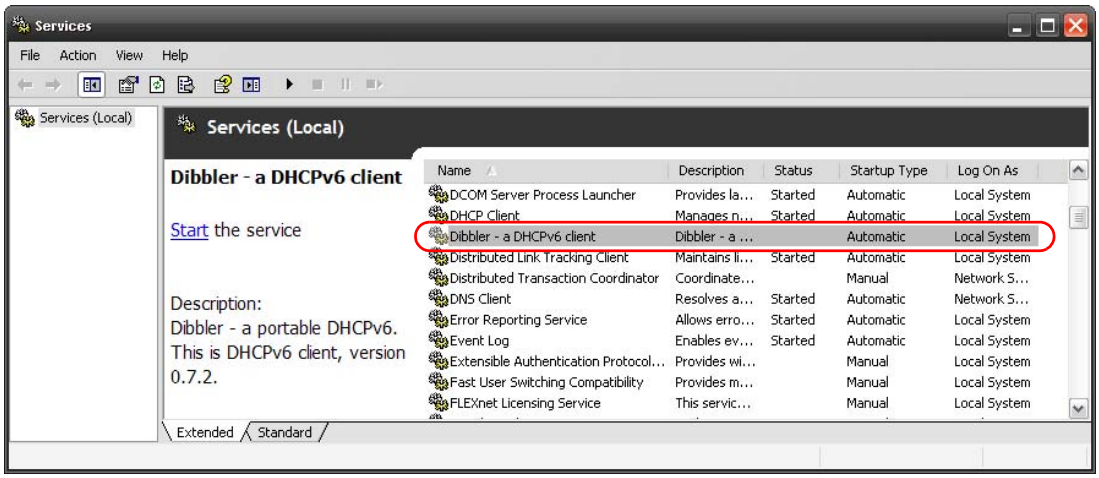
Example - Enabling DHCPv6 on Windows XP

Windows XP does not support DHCPv6. If your network uses DHCPv6 for IP address assignment, you have to additionally install a DHCPv6 client software on your Windows XP. (Note: If you use static IP addresses or Router Advertisement for IPv6 address assignment in your network, ignore this section.)

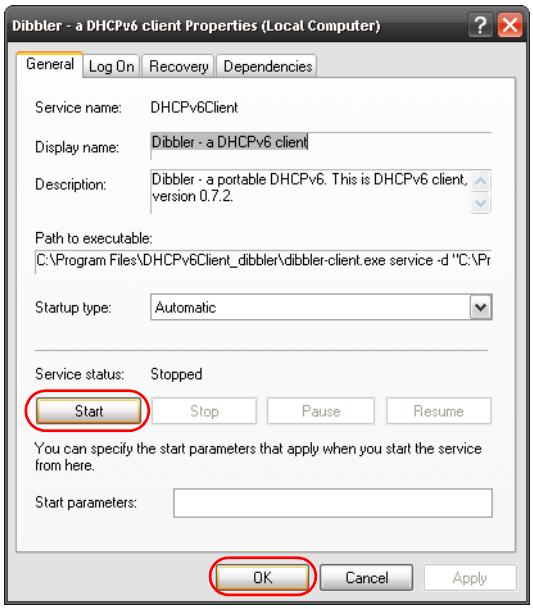
This example uses Dibbler as the DHCPv6 client. To enable DHCPv6 client on your computer:

1. Install Dibbler and select the DHCPv6 client option on your computer.
2. After the installation is complete, select **Start** > **All Programs** > **Dibbler-DHCPv6** > **Client Install as service**.
3. Select **Start** > **Control Panel** > **Administrative Tools** > **Services**.

4 Double click **Dibbler - a DHCPv6 client**.



5 Click **Start** and then **OK**.



6 Now your computer can obtain an IPv6 address from a DHCPv6 server.

Example - Enabling IPv6 on Windows 7

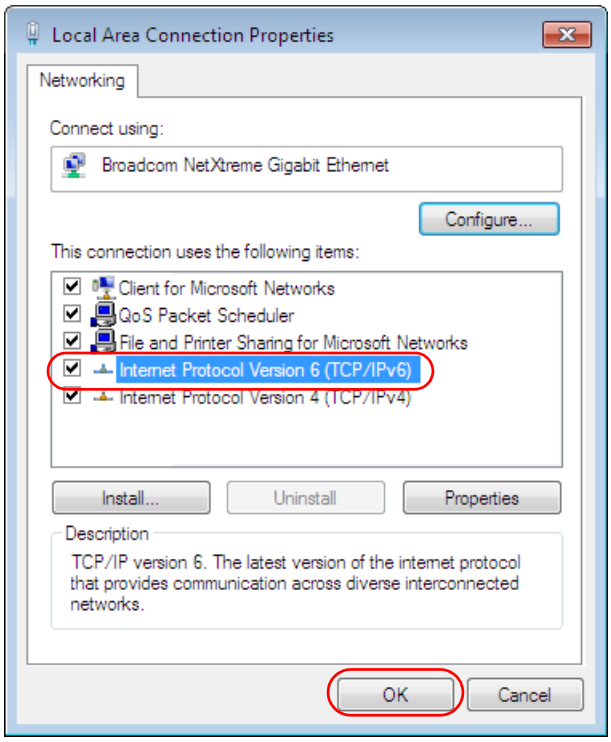
Windows 7 supports IPv6 by default. DHCPv6 is also enabled when you enable IPv6 on a Windows 7 computer.

To enable IPv6 in Windows 7:

1 Select **Control Panel** > **Network and Sharing Center** > **Local Area Connection**.

2 Select the **Internet Protocol Version 6 (TCP/IPv6)** checkbox to enable it.

3 Click **OK** to save the change.



4 Click **Close** to exit the **Local Area Connection Status** screen.

5 Select **Start** > **All Programs** > **Accessories** > **Command Prompt**.

6 Use the `ipconfig` command to check your dynamic IPv6 address. This example shows a global address (`2001:b021:2d::1000`) obtained from a DHCP server.

```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:b021:2d::1000
   Link-local IPv6 Address . . . . . : fe80::25d8:dcab:c80a:5189%11
   IPv4 Address. . . . . . . . . . . : 172.16.100.61
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::213:49ff:feaa:7125%11
                                       172.16.100.254
```

D

Legal Information

Copyright

Copyright © 2015 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Regulatory Notice and Statement (Class A)

United States of America

Federal Communications Commission (FCC) EMC Statement

- This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference.

(2) This device must accept any interference received, including interference that may cause undesired operations.

- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
- This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Canada

The following information applies if you use the product within Canada area

Industry Canada ICES statement

CAN ICES-3 (A)/NMB-3(A)

European Union

The following information applies if you use the product within the European Union.

CE EMC statement

This is Class A Product. In domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

List of National Codes

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Malta	MT
Belgium	BE	Netherlands	NL
Cyprus	CY	Poland	PL
Czech Republic	CR	Portugal	PT
Denmark	DK	Slovakia	SK
Estonia	EE	Slovenia	SI
Finland	FI	Spain	ES
France	FR	Sweden	SE
Germany	DE	United Kingdom	GB
Greece	GR	Iceland	IS
Hungary	HU	Liechtenstein	LI
Ireland	IE	Norway	NO
Italy	IT	Switzerland	CH
Latvia	LV	Bulgaria	BG
Lithuania	LT	Romania	RO
Luxembourg	LU	Turkey	TR

Notices

CLASS 1 LASER PRODUCT

APPAREIL À LASER DE CLASS 1

PRODUCT COMPLIES WITH 21 CFR 1040.10 AND 1040.11.

PRODUIT CONFORME SELON 21 CFR 1040.10 ET 1040.11.

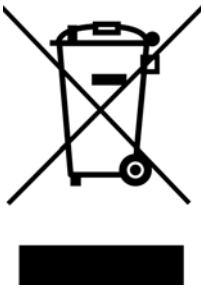
Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Do not obstruct the device ventillation slots as insufficient airflow may harm your device.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Use ONLY power wires of the appropriate wire gauge for your device. Connect it to a power supply of the correct voltage.
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Fuse Warning! Replace a fuse only with a fuse of the same type and rating.
- The POE (Power over Ethernet) devices that supply or receive power and their connected Ethernet cables must all be completely indoors.

Environment Statment

WEEE Directive

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.



"INFORMAZIONI AGLI UTENTI"

Ai sensi della Direttiva 2012/19/UE del Parlamento europeo e del Consiglio, del 4 luglio 2012, sui rifiuti di apparecchiature elettriche ed elettroniche (RAEE)

Il simbolo del cassonetto barrato riportato sull'apparecchiatura o sulla sua confezione indica che il prodotto alla fine della propria vita utile deve essere raccolto separatamente dagli altri rifiuti.

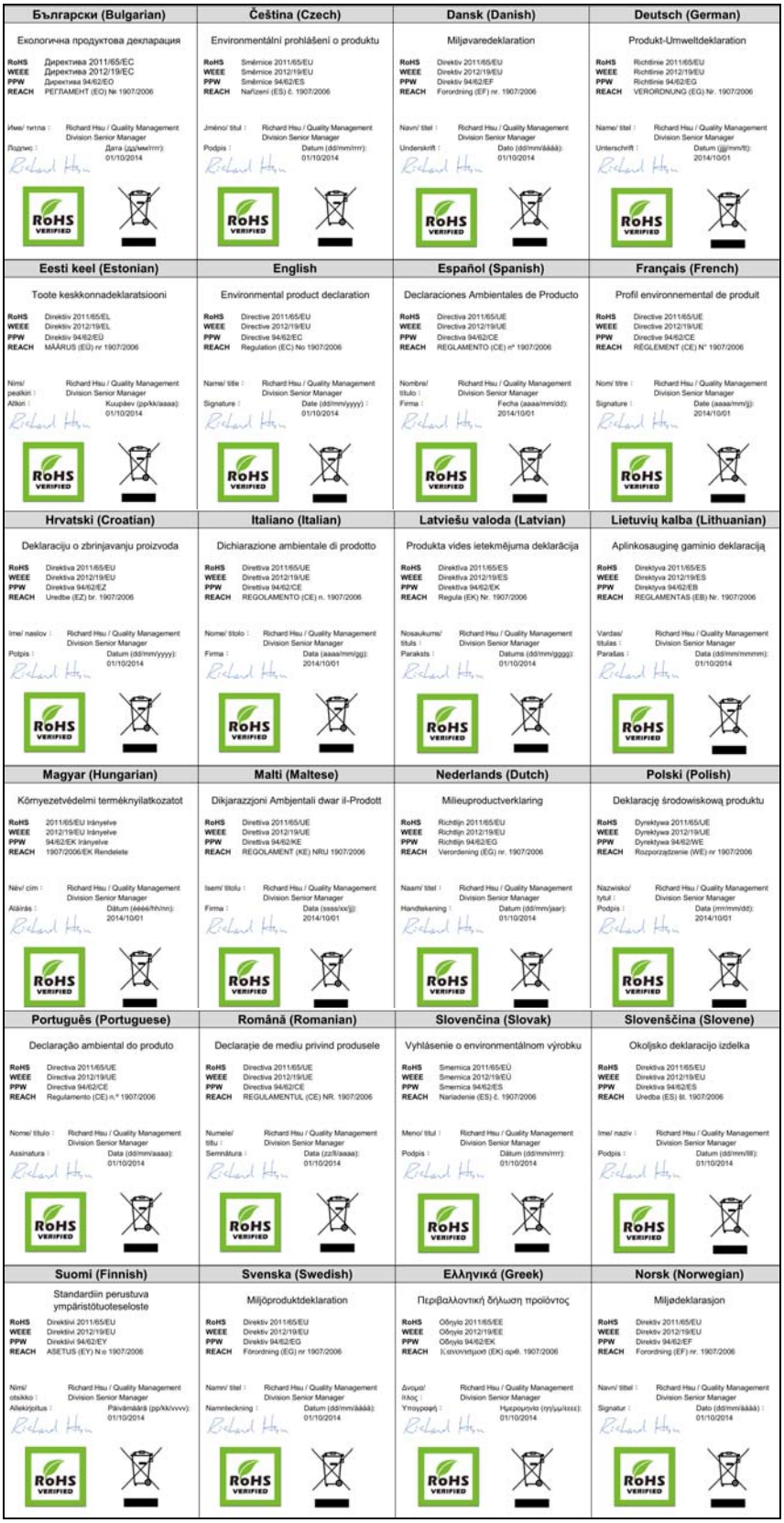
La raccolta differenziata della presente apparecchiatura giunta a fine vita è organizzata e gestita dal produttore. L'utente che vorrà disfarsi della presente apparecchiatura dovrà quindi contattare il

produttore e seguire il sistema che questo ha adottato per consentire la raccolta separata dell'apparecchiatura giunta a fine vita.

L'adeguata raccolta differenziata per l'avvio successivo dell'apparecchiatura dismessa al riciclaggio, al trattamento e allo smaltimento ambientalmente compatibile contribuisce ad evitare possibili effetti negativi sull'ambiente e sulla salute e favorisce il reimpiego e/o riciclo dei materiali di cui è composta l'apparecchiatura.

Lo smaltimento abusivo del prodotto da parte del detentore comporta l'applicazione delle sanzioni amministrative previste dalla normativa vigente."

Environmental Product Declaration


Български (Bulgarian)
Екологична продуктова декларация
RoHS Директива 2011/65/ЕС
WEEE Директива 2012/19/ЕС
PPW Директива 94/62/ЕО
REACH РЕГЛАМЕНТ (ЕО) № 1907/2006
Име/ титла : Richard Hsu / Quality Management Division Senior Manager
Подпис : Дата (дд/мм/гггг): 01/10/2014
Čeština (Czech)
Environmentální prohlášení o produktu
RoHS Směrnice 2011/65/EU
WEEE Směrnice 2012/19/EU
PPW Směrnice 94/62/ES
REACH Nařízení (ES) č. 1907/2006
Jméno/ titul : Richard Hsu / Quality Management Division Senior Manager
Podpis : Datum (dd/mm/rrrr): 01/10/2014
Dansk (Danish)
Miljøvaredeklaration
RoHS Direktiv 2011/65/EU
WEEE Direktiv 2012/19/EU
PPW Direktiv 94/62/EF
REACH Forordning (EF) nr. 1907/2006
Navn/ titel : Richard Hsu / Quality Management Division Senior Manager
Underskrift : Dato (dd/mm/åååå): 01/10/2014
Deutsch (German)
Produkt-Umweltdeklaration
RoHS Richtlinie 2011/65/EU
WEEE Richtlinie 2012/19/EU
PPW Richtlinie 94/62/EG
REACH VERORDNUNG (EG) Nr. 1907/2006
Name/ titel : Richard Hsu / Quality Management Division Senior Manager
Unterschrift : Datum (jjjj/mm/tt): 2014/10/01
Eesti keel (Estonian)
Toote keskkonnadeklaratsiooni
RoHS Direktiiv 2011/65/EL
WEEE Direktiiv 2012/19/EL
PPW Direktiiv 94/62/EÜ
REACH MÄÄRUS (EÜ) nr 1907/2006
Nimi/ ametikoht : Richard Hsu / Quality Management Division Senior Manager
Allkiri : Kuupäev (pp/kk/aaaa): 01/10/2014
English
Environmental product declaration
RoHS Directive 2011/65/EU
WEEE Directive 2012/19/EU
PPW Directive 94/62/EC
REACH Regulation (EC) No 1907/2006
Name/ title : Richard Hsu / Quality Management Division Senior Manager
Signature : Date (dd/mm/yyyy) : 01/10/2014
Español (Spanish)
Declaraciones Ambientales de Producto
RoHS Directiva 2011/65/UE
WEEE Directiva 2012/19/UE
PPW Directiva 94/62/CE
REACH REGLAMENTO (CE) nº 1907/2006
Nombre/ título : Richard Hsu / Quality Management Division Senior Manager
Firma : Fecha (aaaa/mm/dd): 2014/10/01
Français (French)
Profil environnemental de produit
RoHS Directive 2011/65/UE
WEEE Directive 2012/19/UE
PPW Directive 94/62/CE
REACH RÈGLEMENT (CE) N° 1907/2006
Nom/ titre : Richard Hsu / Quality Management Division Senior Manager
Signature : Date (aaaa/mm/jj): 2014/10/01
Hrvatski (Croatian)
Deklaraciju o zbrinjavanju proizvoda
RoHS Direktiva 2011/65/EU
WEEE Direktiva 2012/19/EU
PPW Direktiva 94/62/EZ
REACH Uredba (EZ) br. 1907/2006
Ime/ naslov : Richard Hsu / Quality Management Division Senior Manager
Potpis : Datum (dd/mm/yyyy): 01/10/2014
Italiano (Italian)
Dichiarazione ambientale di prodotto
RoHS Direttiva 2011/65/UE
WEEE Direttiva 2012/19/UE
PPW Direttiva 94/62/CE
REACH REGOLAMENTO (CE) n. 1907/2006
Nome/ titolo : Richard Hsu / Quality Management Division Senior Manager
Firma : Data (aaaa/mm/gg): 2014/10/01
Latviešu valoda (Latvian)
Produkta vides ietekmējuma deklarācija
RoHS Direktīva 2011/65/ES
WEEE Direktīva 2012/19/ES
PPW Direktīva 94/62/EK
REACH Regula (EK) Nr. 1907/2006
Nosaukums/ tituls : Richard Hsu / Quality Management Division Senior Manager
Paraksts : Datums (dd/mm/gggg): 01/10/2014
Lietuvių kalba (Lithuanian)
Aplinkosauginę gaminio deklaraciją
RoHS Direktyva 2011/65/ES
WEEE Direktyva 2012/19/ES
PPW Direktyva 94/62/EB
REACH REGLAMENTAS (EB) Nr. 1907/2006
Vardas/ titulas : Richard Hsu / Quality Management Division Senior Manager
Parašas : Data (dd/mm/mmmm): 01/10/2014
Magyar (Hungarian)
Környezetvédelmi terméknyilatkozatot
RoHS 2011/65/EU Irányelve
WEEE 2012/19/EU Irányelve
PPW 94/62/EK Irányelve
REACH 1907/2006/EK Rendelete
Név/ cím : Richard Hsu / Quality Management Division Senior Manager
Aláírás : Dátum (éééé/hh/nn): 2014/10/01
Malti (Maltese)
Dikjarazzjoni Ambjentali dwar il-Prodott
RoHS Direttiva 2011/65/UE
WEEE Direttiva 2012/19/UE
PPW Direttiva 94/62/KE
REACH REGOLAMENT (KE) NRU 1907/2006
Isem/ titolu : Richard Hsu / Quality Management Division Senior Manager
Firma : Data (ssss/xx/jj): 2014/10/01
Nederlands (Dutch)
Milieuproductverklaring
RoHS Richtlijn 2011/65/EU
WEEE Richtlijn 2012/19/EU
PPW Richtlijn 94/62/EG
REACH Verordening (EG) nr. 1907/2006
Naam/ titel : Richard Hsu / Quality Management Division Senior Manager
Handtekening : Datum (dd/mm/jaar): 01/10/2014
Polski (Polish)
Deklarację środowiskową produktu
RoHS Dyrektywa 2011/65/UE
WEEE Dyrektywa 2012/19/UE
PPW Dyrektywa 94/62/WE
REACH Rozporządzenie (WE) nr 1907/2006
Nazwisko/ tytuł : Richard Hsu / Quality Management Division Senior Manager
Podpis : Data (rr/mm/dd): 2014/10/01
Português (Portuguese)
Declaração ambiental do produto
RoHS Directiva 2011/65/UE
WEEE Directiva 2012/19/UE
PPW Directiva 94/62/CE
REACH Regulamento (CE) n.º 1907/2006
Nome/ título : Richard Hsu / Quality Management Division Senior Manager
Assinatura : Data (dd/mm/aaaa): 01/10/2014
Română (Romanian)
Declarație de mediu privind produsele
RoHS Directiva 2011/65/UE
WEEE Directiva 2012/19/UE
PPW Directiva 94/62/CE
REACH REGULAMENTUL (CE) NR. 1907/2006
Numele/ titlu : Richard Hsu / Quality Management Division Senior Manager
Semnătura : Data (zz/ll/aaaa): 01/10/2014
Slovenčina (Slovak)
Vyhlásenie o environmentálnom výrobku
RoHS Smernica 2011/65/EÚ
WEEE Smernica 2012/19/EÚ
PPW Smernica 94/62/ES
REACH Nariadenie (ES) č. 1907/2006
Meno/ titul : Richard Hsu / Quality Management Division Senior Manager
Podpis : Dátum (dd/mm/rrrr): 01/10/2014
Slovenščina (Slovene)
Okoljsko deklaracijo izdelka
RoHS Direktiva 2011/65/EU
WEEE Direktiva 2012/19/EU
PPW Direktiva 94/62/ES
REACH Uredba (ES) št. 1907/2006
Ime/ naziv : Richard Hsu / Quality Management Division Senior Manager
Podpis : Datum (dd/mm/llll): 01/10/2014
Suomi (Finnish)
Standardiin perustuva ympäristötuoteseloste
RoHS Direktiivi 2011/65/EU
WEEE Direktiivi 2012/19/EU
PPW Direktiivi 94/62/EY
REACH ASETUS (EY) N:o 1907/2006
Nimi/ otsikko : Richard Hsu / Quality Management Division Senior Manager
Allekirjoitus : Päivämäärä (pp/kk/vvvv): 01/10/2014
Svenska (Swedish)
Miljöproduktdeklaration
RoHS Direktiv 2011/65/EU
WEEE Direktiv 2012/19/EU
PPW Direktiv 94/62/EG
REACH Förordning (EG) nr 1907/2006
Namn/ titel : Richard Hsu / Quality Management Division Senior Manager
Namnteckning : Datum (dd/mm/åååå): 01/10/2014
Ελληνικά (Greek)
Περιβαλλοντική δήλωση προϊόντος
RoHS Οδηγία 2011/65/ΕΕ
WEEE Οδηγία 2012/19/ΕΕ
PPW Οδηγία 94/62/ΕΚ
REACH Κανονισμού (ΕΚ) αριθ. 1907/2006
Όνομα/ τίτλος : Richard Hsu / Quality Management Division Senior Manager
Υπογραφή : Ημερομηνία (ηη/μμ/εεεε): 01/10/2014
Norsk (Norwegian)
Miljødeklarasjon
RoHS Direktiv 2011/65/EU
WEEE Direktiv 2012/19/EU
PPW Direktiv 94/62/EF
REACH Forordning (EF) nr. 1907/2006
Navn/ tittel : Richard Hsu / Quality Management Division Senior Manager
Signatur : Dato (dd/mm/åååå) : 01/10/2014

Taiwanese BSMI (Bureau of Standards, Metrology and Inspection) A Warning:

警告使用者
這是甲類的資訊產品，在居住的環境使用時，
可能造成射頻干擾，在這種情況下，
使用者會被要求採取某些適當的對策.

Viewing Certifications

Go to http://www.zyxel.com to view this product's documentation and certifications.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized ZyXEL local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Trademarks

ZyNOS (ZyXEL Network Operating System) and ZON (ZyXEL One Network)are registered trademarks of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Open Source Licenses

This product contains in part some free software distributed under GPL license terms and/or GPL like licenses. Open source licenses are provided with the firmware package. You can download the latest firmware at www.zyxel.com. To obtain the source code covered under those Licenses, please contact support@zyxel.com.tw to get it.

Index

Numerics

802.1P priority 70
802.3az 264

A

AAA 201
AAA (Authentication and Authorization) 201
access control
  limitations 327
  login account 332
  remote management 335
  service port 334
  SNMP 336
address learning, MAC 97, 99
Address Resolution Protocol (ARP) 313, 360, 364, 365
administrator password 333
age 127
aggregator ID 142, 144
airflow 28
applications
  backbone 18
  bridging 19
  IEEE 802.1Q VLAN 20
  switched workgroup 19
ARP
  how it works 313
ARP (Address Resolution Protocol) 313, 360
ARP inspection 213, 233
  and MAC filter 233
  configuring 234
  syslog messages 234
  trusted ports 234
ARP Table 360
authentication 201
  setup 206
Authentication and Authorization, see AAA 201
authorization 201
  setup 206
automatic VLAN registration 87

B

back up, configuration file 321
bandwidth control 134
  egress rate 135
  ingress rate 135
  setup 134
basic settings 58
basic setup tutorial 43
binding 212
binding table 212
  building 213
BPDUs (Bridge Protocol Data Units) 116
Bridge Protocol Data Units (BPDUs) 116
broadcast storm control 136

C

CDP 241
certifications
  notices 391
  viewing 394
CFI (Canonical Format Indicator) 87
changing the password 37
Cisco Discovery Protocol, see CDP
CIST 133
Class of Service (CoS) 296
classifier 162, 166
  and QoS 162
  editing 167
  example 169
  overview 162
  setup 162, 166, 167
  viewing 167
cloning a port See port cloning

cluster management 349
and switch passwords 352
cluster manager 349, 352
cluster member 349, 352
cluster member firmware upgrade 353
network example 349
setup 351
specification 349
status 350
switch models 349
VID 352
web configurator 353
cluster manager 349
cluster member 349
Common and Internal Spanning Tree, See CIST 133
configuration 294
change running config 322
configuration file
backup 321
restore 320
saving 322
configuration, saving 37
contact information 373
copying port settings, See port cloning
copyright 390
CPU history 324
CPU management port 103
CPU protection
configuration 254
overview 254
CPU threshold 323
crash log report 324
current date 62
current time 61
customer support 373

D

daylight saving time 62
default Ethernet settings 26
DHCP
configuration options 300
relay example 310
setup 308
DHCP relay option 82 232
DHCP snooping 43, 213, 231
configuring 232
DHCP relay option 82 232
trusted ports 231
untrusted ports 231
DHCP snooping database 232
diagnostics 344
Ethernet port test 345
ping 345
system log 345
Differentiated Service (DiffServ) 296
DiffServ 296
activate 297
DS field 296
DSCP 296
network example 297
PHB 297
disclaimer 390
DS (Differentiated Services) 296
DSCP
service level 296
what it does 297
DSCP (DiffServ Code Point) 296
dynamic link aggregation 140

E

EEE 264
egress port 105
egress rate, and bandwidth control 135
Energy Efficient Ethernet 264
erase running-configuration 321
error disable detect 252, 255
error disable recovery
configuration 256
overview 256
Ethernet broadcast address 313, 360
Ethernet port test 345
external authentication server 202

F

factory defaults 322

fan speed 60
FCC interference statement 390
file transfer using FTP
  command example 324
filename convention, configuration
  configuration
    file names 324
Filtering 193
filtering 113
  rules 113
filtering database, MAC table 355
Filtering Profile 194
firmware 59
  upgrade 319, 353
flow control 70
  back pressure 70
  IEEE802.3x 70
forwarding
  delay 127
frames
  tagged 96
  untagged 96
front panel 25
FTP 324
  file transfer procedure 325
  restrictions over WAN 326

G

GARP 87
GARP (Generic Attribute Registration Protocol) 87
GARP terminology 88
GARP timer 63, 64, 87
general setup 60
getting help 38
Gigabit ports 25
GMT (Greenwich Mean Time) 62
Green Ethernet 264
GVRP 88, 95
  and port assignment 95
GVRP (GARP VLAN Registration Protocol) 88

H

hardware installation 22
hardware monitor 60
hardware overview 25
hello time 127
hops 127
HTTPS 339
  certificates 339
  implementation 339
  public keys, private keys 339
HTTPS example 340

I

IEEE 802.1p, priority 64
IEEE 802.1x
  activate 150, 153, 204
  reauthentication 151
IEEE 802.1x, port authentication 148
IGMP filtering
  profile 187
IGMP leave timeout
  fast 185
  mormal 184
IGMP snooping 178
  MVR 180
IGMP throttling 185
ingress port 105
ingress rate, and bandwidth control 135
installation
  desktop 22
  precautions 22
  rack-mounting 22
  transceivers 26
installation scenarios 22
Internet Protocol version 6, see IPv6
IP
  routing domain 67
IP address 65, 66, 68
IP setup 65
IP source guard 212, 213
  ARP inspection 213, 233
  DHCP snooping 213, 231

static bindings 213
IP subnet mask 65, 66, 67, 68
IP Table 358
IP table 358
how it works 358
IPv6 382
addressing 382
EUI-64 384
global address 383
interface ID 384
link-local address 382
Neighbor Discovery Protocol 382
ping 382
prefix 382
prefix length 382
stateless autoconfiguration 384
unspecified address 383
IPv6 neighbor table 367
IPv6 static route
configuration 294

L

L2PT 239
access port 240
CDP 239
configuration 240
encapsulation 239
LACP 239
MAC address 239
mode 240
overview 239
PAgP 239
point to point 239
STP 239
tunnel port 240
UDLD 239
VTP 239
LACP 140, 242
system priority 145
timeout 146
Layer 2 protocol tunneling, see L2PT
LEDs 29
limit MAC address learning 158
link aggregation 140
dynamic 140
ID information 141
setup 142, 144
status 142
traffic distribution algorithm 142
traffic distribution type 144
trunk group 140
Link Aggregation Control Protocol (LACP) 140
Link Aggregation Control Protocol, see LACP 140
Link Layer Discovery Protocol (LLDP) 266, 267
LLDP (Link Layer Discovery Protocol) 266
LLDP-MED (Link Layer Discovery Protocol for Media Endpoint Devices) 267
lockout 37
log 345
login 32
password 37
login account
Administrator 332
non-administrator 333
login accounts 332
configuring via web configurator 332
multiple 332
number of 332
login password 333
loop guard 235
examples 236
port shut down 237
setup 237
vs. STP 235

M

MAC (Media Access Control) 59
MAC address 59, 313, 360
maximum number per port 158, 159
MAC address learning 63, 97, 99, 108, 158
specify limit 158
MAC authentication 149
aging time 154
MAC filter
and ARP inspection 233
MAC freeze 157
MAC table 355
display criteria 357
how it works 355

sorting criteria 357
transfer type 357
viewing 356
MAC-based VLAN 102
maintanence
configuration backup 321
firmware 319
restoring configuration 320
maintenance 318
current configuration 318
main screen 318
Management Information Base (MIB) 337
management port 105
managing the device
good habits 21
using FTP. See FTP. 21
man-in-the-middle attacks 233
max
age 127
hops 127
maximum transmission unit 363
mbuf (Memory Buffer) 323
memory section log 324
MIB
and SNMP 337
supported MIBs 337
MIB (Management Information Base) 337
mini GBIC ports 26
connection speed 26
connector type 26
mirroring ports 138
MLD Snooping-proxy 189
monitor port 138, 139
mounting brackets 23
MRSTP status 124
MSA (MultiSource Agreement) 26
MST ID 133
MST Instance, See MSTI 133
MST region 132
MSTI 133
MSTP 115, 117
bridge ID 130, 131
configuration 125
configuration digest 131
forwarding delay 127
Hello Time 130
hello time 127
Max Age 130
max age 127
max hops 127
path cost 128
port priority 128
revision level 127
status 129
MTU 363
MTU (Multi-Tenant Unit) 62
multicast
IGMP throttling 185
IP addresses 178
setup 183, 189, 191, 193
multicast group 187
multicast VLAN 197
Multiple Rapid Spanning Tree Protocol 117
Multiple RSTP 117
Multiple Spanning Tree Protocol, See MSTP 115, 117
Multiple STP 117
MVR 180
configuration 195
group configuration 197
network example 180
MVR (Multicast VLAN Registration) 180

N

network applications 18
network management system (NMS) 336
NTP (RFC-1305) 61

P

PAGP 242
password 37
administrator 333
Path MTU 363
Path MTU Discovery 363
PHB (Per-Hop Behavior) 297
ping, test connection 345
policy 172
and classifier 172

and DiffServ 171
configuration 172
overview 171
rules 171
viewing 174
Port Aggregation Protocol, see PAgP
port authentication 148
and RADIUS 202
IEEE802.1x 150, 153, 204
MAC authentication 149
port based VLAN type 63
port cloning 364, 365
advanced settings 364, 365
basic settings 364, 365
port details 54
port isolation 105
port mirroring 138, 139
direction 139
egress 139
ingress 139
port redundancy 140
Port Role 191
port security 156, 160
limit MAC address learning 158
MAC address learning 156, 160
overview 156, 160
setup 156, 160, 237, 240
port setup 69
port status 53
port VLAN ID, see PVID 95
port VLAN trunking 88
port-based VLAN 103
all connected 105
port isolation 105
settings wizard 105
ports
diagnostics 345
mirroring 138
speed/duplex 70
standby 141
power
voltage 60
power connector 28
power status 60
PPPoE IA
trusted ports 245
untrusted ports 245
priority level 64
priority, queue assignment 64
private VLAN status 91
probe 368
product registration 394
protocol based VLAN 98
and IEEE 802.1Q tagging 98
application example 99
configuration example 106
isolate traffic 98
priority 100
un-tagged packets 98
PVID 87
PVID (Priority Frame) 87

Q

QoS
and classifier 162
queue weight 176
queuing 175
SPQ 175
WRR 175
queuing method 175, 177

R

rack-mounting 22
RADIUS 201, 202
advantages 202
and port authentication 202
and tunnel protocol attribute 209
Network example 201
server 202
settings 202
setup 202
Rapid Spanning Tree Protocol, See RSTP. 115
reachable 368
Read Only Memory (ROM) 324
rear panel connections 28
reboot
load configuration 322
reboot system 322

registration
product 394
remote management 335
service 336
trusted computers 336
resetting 38, 321, 322
to factory default settings 321, 322
restoring configuration 38, 320
RFC 3164 346
Round Robin Scheduling 175
route information 362
routing domain 67
routing table 362
RSTP 115

S

save configuration 37, 322
service access control 334
service port 334
Simple Network Management Protocol, see SNMP
SNMP 336
agent 337
and MIB 337
authentication 332
communities 328
management model 336
manager 337
MIB 337
network components 336
object variables 337
protocol operations 337
security 331, 332
setup 328
traps 329
users 331
version 3 and security 337
versions supported 336
SNMP traps 338
supported 338
Spanning Tree Protocol, See STP. 115
SPQ (Strict Priority Queuing) 175
SSL (Secure Socket Layer) 339
stale 368
standby ports 141
static bindings 213
static link aggregation example 146
static MAC address 108
static MAC forwarding 97, 99, 108
static multicast address 110
static multicast forwarding 110
static route
overview 291
static routes 294
static trunking example 146
Static VLAN 92
static VLAN
control 94
tagging 94
status 33, 53
link aggregation 142
MSTP 129
port 53
port details 54
power 60
STP 121, 124
VLAN 89
STP 115, 241
bridge ID 121, 125
bridge priority 120, 123
configuration 119, 122
designated bridge 116
forwarding delay 120, 124
Hello BPDU 116
Hello Time 120, 121, 124, 125
how it works 116
Max Age 120, 121, 124, 125
path cost 116, 121, 124
port priority 120, 124
port state 117
root port 116
status 121, 124
terminology 116
vs. loop guard 235
subnet based VLAN 98
and DHCP VLAN 98
priority 98
setup 97
subnet based VLANs 96
switch lockout 37
switch reset 38
switch setup 63

syslog 234, 346
  protocol 346
  server setup 347
  settings 346
  setup 346
  severity levels 346
system information 58, 71, 72
system log 345
system reboot 322

T

TACACS+ 201, 202
  setup 204
TACACS+ (Terminal Access Controller Access-Control System Plus) 201
tagged VLAN 86
Tech-Support 323
tech-support 323
temperature indicator 60
time
  current 61
  time zone 62
Time (RFC-868) 61
time server 61
time service protocol 61
  format 61
trademarks 394
transceivers
  installation 26
  removal 27
traps
  destination 329
trunk group 140
trunking 140
  example 146
trusted ports
  ARP inspection 234
  DHCP snooping 231
  PPPoE IA 245
tunnel protocol attribute, and RADIUS 209
tutorials 43
  DHCP snooping 43
Type of Service (ToS) 296

U

UDLD 242
UniDirectional Link Detection, see UDLD
untrusted ports
  ARP inspection 234
  DHCP snooping 231
  PPPoE IA 245
user profiles 202

V

Vendor Specific Attribute, See VSA 208
ventilation 22
VID 90
  number of possible VIDs 87
  priority frame 87
VID (VLAN Identifier) 87
VLAN 62
  acceptable frame type 96
  automatic registration 87
  ID 86
  ingress filtering 95
  introduction 62, 86
  number of VLANs 89
  port number 90
  port settings 94
  port-based VLAN 103
  port-based, all connected 105
  port-based, isolation 105
  port-based, wizard 105
  private VLAN 91
  PVID 95
  static VLAN 92
  status 89, 90, 91
  subnet based 96
  tagged 86
  trunking 88, 96
  type 63, 89
VLAN (Virtual Local Area Network) 62
VLAN number 65, 66, 68
VLAN Trunking Protocol, see VTP
VLAN, protocol based, See protocol based VLAN 98
Voice VLAN 100
VSA 208

VTP 242

W

warranty 394
  note 394
web configurator 32
  getting help 38
  home 33
  login 32
  logout 38
  navigation panel 34
weight, queuing 176
Weighted Round Robin Scheduling (WRR) 176
WRR (Weighted Round Robin Scheduling) 175

Z

ZON Neighbor Management 52
ZON Utility 51
ZyNOS (ZyXEL Network Operating System) 324